DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL /

DOUTRINA E PRÁTICA EM DEBATE < VOL.1 >

DENNYS ANTONIALLI (ED.)
JACQUELINE DE SOUZA ABREU (ED.)

CARINA QUITO
CAROLINA YUMI DE SOUZA
FRANCISCO BRITO CRUZ
GREG NOJEIM
JULIANO MARANHÃO
MARCOS ZILLI
MARIANA GIORGETTI VALENTE
RIANA PFEFFERKORN
TERCIO SAMPAIO FERRAZ JR.

INTERNETLAB
pesquisa em direito e tecnologia

DIREITOS FUNDAMENTAIS E PROCESSO PENAL NA ERA DIGITAL /

DOUTRINA E PRÁTICA EM DEBATE < VOL.1 >

DENNYS ANTONIALLI (ED.)
JACQUELINE DE SOUZA ABREU (ED.)

CARINA QUITO
CAROLINA YUMI DE SOUZA
FRANCISCO BRITO CRUZ
GREG NOJEIM
JULIANO MARANHÃO
MARCOS ZILLI
MARIANA GIORGETTI VALENTE
RIANA PFEFFERKORN
TERCIO SAMPAIO FERRAZ JR.

SÃO PAULO, 2018

INTERNETLAB
pesquisa em direito e tecnologia

InternetLab é uma organização sem fins lucrativos dedicada à produção de pesquisa acadêmica aplicada com impacto em políticas públicas de tecnologia e Internet no Brasil.

Citação sugerida
ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. I. São Paulo. InternetLab, 2018.

Avenida Ipiranga 344 cj 11B | 01046-010 | São Paulo | SP | Brasil
ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA
www.internetlab.org.br

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Direitos fundamentais e processo penal na era digital / Dennys Antonialli, Jacqueline de Souza Abreu [editores]. -- São Paulo : InternetLab, 2018. -- (Doutrina e prática em debate ; v. 1)

Vários autores.
Bibliografia.
ISBN 978-85-92871-01-7

1. Direito processual penal **2.** Direitos fundamentais **3.** Processo penal **4.** Tecnologia e direito **5.** Tecnologias da informação e comunicação **I.** Antonialli, Dennys. **II.** Abreu, Jacqueline de Souza. **III.** Série.

18-15876 **CDU-343.1:004**

Índices para catálogo sistemático:
1. Direito e tecnologia : Direito processual penal **343.1:004**
Maria Paula C. Riyuzo - Bibliotecária - CRB-8/7639

AUTORES /

< JACQUELINE DE SOUZA ABREU >

Doutoranda em filosofia e teoria geral do direito na Universidade de São Paulo e pesquisadora no InternetLab. É mestra em Direito, com especialização em Direito e Tecnologia, pela Universidade de California, Berkeley (LL.M., 2016) e também, com especialização em Direito Constitucional, pela Universidade Ludwig Maximilian de Munique (LL.M., 2015). É bacharela em Direito pela Universidade de São Paulo (LL.B., 2014). Durante seus estudos, recebeu bolsas de estudo da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e do Serviço Alemão de Intercâmbio Acadêmico (DAAD). Foi membro do Núcleo de Direito, Internet e Sociedade da Faculdade de Direito da USP e assistente de pesquisa no Berkman Center for Internet & Society na Universidade Harvard.

< DENNYS ANTONIALLI >

Professor Doutor do Departamento de Direito do Estado da Faculdade de Direito da Universidade de São Paulo (USP). É doutor e bacharel em direito pela mesma instituição. Possui mestrado em direito pela Stanford Law School (EUA) e mestrado profissional em "Law and Business", conjuntamente oferecido pela Bucerius Law School e pela WHU Otto Beisheim School of Management (Alemanha). Atuou junto à equipe de políticas públicas em tecnologia e direitos civis na American Civil Liberties Union of Northern California (ACLU/NC) e como consultor jurídico do "Timor Leste Legal Education Project", da Agência dos Estados Unidos para De-

senvolvimento Internacional (USAID). Em 2011, foi ganhador do 1º lugar do Steven M. Block Civil Liberties Award, prêmio conferido ao melhor trabalho escrito na área de liberdades públicas da Stanford Law School. Em 2012, foi ganhador do 1º lugar do "Prêmio Marco Civil da Internet e Desenvolvimento" da Escola de Direito da Fundação Getúlio Vargas (FGV-SP). Foi pesquisador associado do Alexander von Humboldt Institute for Internet and Society (Berlim) e fez parte da turma de 2014 do "Summer Doctoral Program" do Oxford Internet Institute (Reino Unido). Em 2016, foi pesquisador visitante da Stanford Law School (EUA), a convite do Prof. Lawrence Friedman. Advogado e autor de diversos artigos e capítulos de livro, desde 2012, é coordenador do Núcleo de Direito, Internet e Sociedade da Faculdade de Direito da Universidade de São Paulo (NDIS-USP). Especialista nas áreas de privacidade e vigilância, Dennys contribuiu com os trabalhos da Comissão Parlamentar de Inquérito de Crimes Cibernéticos e participou de inúmeros eventos nacionais e internacionais.

< FRANCISCO BRITO CRUZ >

Doutorando e mestre em Filosofia e Teoria Geral do Direito na Faculdade de Direito da Universidade de São Paulo (FDUSP). Graduado em Direito pela Faculdade de Direito da Universidade de São Paulo (FDUSP) e, durante o curso, bolsista do Programa de Educação Tutorial (PET) – Sociologia Jurídica. Em 2010, participou do programa de intercâmbio da Secretaria de Assuntos Legislativos (SAL) do Ministério da Justiça e da Secretaria para Assuntos Jurídicos (SAJ) da Casa Civil da Presidência da República. Foi pesquisador visitante (2013) no Center for Study of Law and Society, da Universidade da Califórnia – Berkeley, por meio de programa de intercâmbio da Rede de Pesquisa Em-

pírica em Direito (REED). Em 2011, foi ganhador do 1º lugar do Prêmio Marco Civil da Internet e Desenvolvimento da Escola de Direito da Fundação Getúlio Vargas (SP). Autor de artigos acadêmicos e de opinião sobre políticas de Internet, fundou e é coordenador (2012-2014, 2016-atual) do Núcleo de Direito, Internet e Sociedade da Universidade de São Paulo (NDIS-USP). É especialista no monitoramento de políticas públicas ligadas à tecnologia e pesquisa sobre as relações delas com a democracia.

< TERCIO SAMPAIO FERRAZ JÚNIOR >

Professor aposentado do Departamento de Filosofia e Teoria Geral do Direito na Faculdade de Direito da Universidade de São Paulo (USP) e professor emérito pela Faculdade de Direito da USP em Ribeirão Preto. Advogado sócio de Sampaio Ferraz Advogados. Possui graduação em Filosofia, Letras e Ciências Humanas pela Universidade de São Paulo (1964), graduação em Ciências Jurídicas e Sociais pela Universidade de São Paulo (1964), doutorado em Filosofia - Johannes Gutemberg Universitat de Mainz (1968) e doutorado em Direito pela Universidade de São Paulo (1970).

< MARIANA GIORGETTI VALENTE >

Doutoranda e mestre em Sociologia Jurídica pela USP. Foi pesquisadora visitante na Universidade da Califórnia, Berkeley entre 2016 e 2017. Coordenou, em 2015 e 2016, o Núcleo de Direito, Internet e Sociedade, também na USP (NDIS). Entre 2014 e 2016, foi também pesquisadora e consultora do projeto Acervos Digitais, no Centro de Tecnologia e Sociedade da FGV, onde também co-coordenou o projeto

Open Business Models, sobre direitos autorais e música na era digital (2012-2014), e foi professora do curso Direitos Intelectuais (2014), na graduação em direito. Pela FGV, foi também uma das coordenadoras legais do projeto Creative Commons Brasil. Desde 2008, é membro do Núcleo Direito e Democracia do Centro Brasileiro de Análise e Planejamento (Cebrap), pelo qual foi coautora de pesquisas do programa Pensando o Direito (SAL/MJ), nas áreas áreas de direitos das mulheres, processo legislativo e propriedade intelectual. Graduou-se em Direito pela Universidade de São Paulo em 2009 e tem especialização em propriedade intelectual pela Organização Mundial de Propriedade Intelectual (Summer School, 2011). Foi coordenadora jurídica do Museu de Arte Moderna de São Paulo, e coordena o grupo Direitos Autorais do GT Arquivos de Museus e Pesquisa (Capes).

< JULIANO MARANHÃO >

Professor Associado da Faculdade de Direito da Universidade de São Paulo (USP), onde ingressou em 2007. Possui Bacharelado, Doutorado e Livre-Docência em Direito pela USP (1998, 2004 e 2011). Foi pesquisador visitante nas universidades de Miami, Leipzig e Maastricht. Fez pós-doutorado na Pontifícia Universidade Católica de São Paulo e na Universidade de Utrecht. Membro do Instituto Brasileiro de Filosofia. Coordenador e editor da Revista Brasileira de Filosofia. Tem experiência nas áreas de Direito e de Lógica, com ênfase em teoria do direito, lógica jurídica, lógicas de revisão de crenças, lógica e teoria da argumentação. É coordenador do Núcleo Direito, Incerteza e Tecnologia da Faculdade de Direito da USP.

< GREG NOJEIM >

Advogado e diretor do projeto Liberdade, Segurança e Tecnologia, no Center for Democracy & Technology, em Washington (EUA). Nojeim conduz a maior parte do trabalho do CDT nas áreas de segurança nacional, terrorismo e proteções da Quarta Emenda. Ele é profundamente envolvido no esforço de trazer as proteções de privacidade da Quarta Emenda a comunicações digitais. Ele frequentemente fala no Congresso Nacional estadunidense em audiências públicas sobre questões ligadas a cibersegurança e legislação anti-terrorismo como o Patriot Act. Nojeim foi co-presidente do comitê sobre segurança nacional e liberdades civis da seção de direitos e responsabilidades individuais da American Bar Association. Atualmente, ele também é parte do conselho DHS sobre privacidade e integridade de dados. Antes de se juntar ao CDT em 2007, Nojeim trabalhou no escritório de Washington da American Civil Liberties Union e também como advogado no escritório Kirkpatrick & Lockhart, onde se especializou em fusões e aquisições, valores mobiliários e comércio internacional.

< RIANA PFEFFERKORN >

Cryptography Fellow no Stanford Center for Internet and Society. Seu trabalho foca na análise das políticas e práticas do governo estadunidense em forçar e desencriptação e influenciar o desenho de plataformas, serviços, aparelhos e produtos quando à criptografia, seja por meios tecnológicos, judiciais ou legislativos. Riana também pesquisa os benefícios e malefícios da criptografia forte para a liberdade de expressão, o engajamento político, o desenvolvimento econômico e outros interesses públicos. Antes de se juntar a

Stanford, Riana foi advogada associada no escritório Wilson Sonsini Goodrich & Rosati, onde trabalhou com contencioso e consultivo nas áreas de responsabilidade de intermediários na internet, proteção ao consumidor, direito autoral, marcas, e segredo industrial. Antes disso, Riana foi assistente judiciária do Juiz Bruce J. McGiverin do tribunal distrital em Porto Rico. Ela também estagiou com o Juiz Stephen Reinhardt do Tribunal de Apelações do Nono Circuito. Riana obteve seu diploma em direito na Faculdade de Direito da Universidade de Washington.

< CAROLINA YUMI DE SOUZA >

Advogada Geral da União. Doutora e mestre em Processo Penal pela Universidade de São Paulo. Possui mestrado em Direito Processual pela Universidade de São Paulo (2006). Tem experiência e publicações na área de cooperação jurídica internacional.

< CARINA QUITO >

Advogada criminalista, sócia de Sica & Quito Advogados. Mestre em Direito Processual Penal pela Universidade de São Paulo.

< MARCOS ZILLI >

Juiz Titular de Direito da 15ª Vara Criminal de São Paulo. Professor Dr. de Direito Processual Penal nos cursos de graduação e de pós-graduação da Faculdade de Direito da Universidade de São Paulo (USP). Mestre e Doutor em Direito Processual pela mesma Universidade. Especialista em

Direito Penal Econômico e Europeu pela Faculdade de Direito da Universidade de Coimbra e pelo Instituto Brasileiro de Ciências Criminais (IBCCrim). Professor do Curso de Pós-graduação Interdisciplinar Humanidades, Direitos e outras Legitimidades da Faculdade de Filosofia, Letras e Ciências Humanas da Universidade de São Paulo (USP). Membro do Grupo Latino-americano de Estudos de Direito Penal Internacional promovido pela Fundação Konrad Adenauer. Membro do Diversitas, Núcleo de Estudos das Diversidades, Intolerâncias e Conflitos da Universidade de São Paulo (USP). Membro do Forum for International Criminal and Humanitarian Law (FICHL). Coordenador Editorial da Coleção Fórum de Direitos Humanos. Consultor da International Nuremberg Principles Academy. Membro Consultor da Comissão Especial de Política Criminal e Penitenciária da OAB/SP - Portaria 449/16/PR.

SUMÁRIO /

APRESENTAÇÃO DOS EDITORES /

Não há dúvidas de que as novas tecnologias de comunicação e informação revolucionaram as atividades de investigação criminal. De aplicativos de mensagens munidos de tecnologias de criptografia forte a serviços de hospedagem em nuvem, o dia-a-dia das autoridades de investigação passou a envolver não somente novas fontes de prova como também novas questões a respeito de suas possibilidades de obtenção e utilização para fins de instrução processual.

Foi pensando nesse contexto que o InternetLab, centro independente de pesquisa em direito e tecnologia, com apoio institucional da Faculdade de Direito da Universidade de São Paulo (FDUSP), realizou entre os dias 29 e 31 de maio de 2017 o I Congresso Internacional "Direitos Fundamentais e Processo Penal na Era Digital".

Reunindo renomados juristas e especialistas nas áreas de privacidade e segurança, nacionais e internacionais, o congresso promoveu o debate sobre as garantias do efetivo processo penal e a tutela de direitos fundamentais como os direitos à privacidade e ao sigilo das comunicações em face das novas tecnologias.

As palestras, sessões e mesa redonda discutiram temas como as possibilidades de acesso a dados e conteúdo de comunicações, busca e apreensão de dispositivos eletrônicos, desafios relacionados à cooperação jurídica internacional para acesso a evidências digitais, tecnologias de segurança e criptografia, entre outros.

Os vídeos de todos os painéis podem ser assistidos no canal do InternetLab no Youtube.

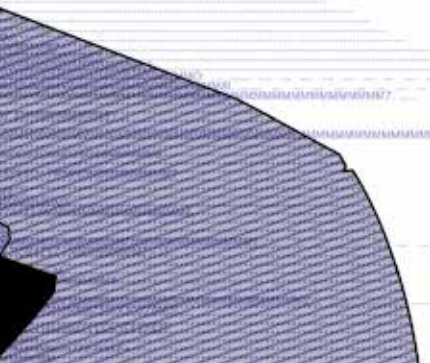
Após o congresso, os palestrantes foram convidados a submeter versões escritas de suas contribuições ou a autorizar a transcrição de suas apresentações. O resultado deste trabalho consiste nesta publicação, que além de retratar em detalhes grande parte das discussões iniciadas durante o congresso, contribui para o aprofundamento e atualização das doutrinas jurídicas que se propõem a guiar os operadores do direito processual penal na era digital.

DENNYS ANTONIALLI
JACQUELINE DE SOUZA ABREU
São Paulo, dezembro de 2017

01.

SIGILO DE DADOS, O DIREITO À PRIVACIDADE E OS LIMITES DO PODER DO ESTADO: 25 ANOS DEPOIS

Tércio Sampaio Ferraz Jr.



Transcrição da palestra feita por Heloísa Massaro. Editado por Jacqueline de Souza Abreu. Revisado por Juliano Maranhão.

A Faculdade de Direito do Largo de São Francisco faz 190 anos e eu já estou na faculdade há 57. Quando eu ouço que o artigo "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado"[1] ainda está assim vivo me surpreende que, destes 190, ele tem 25. Olhando esses números me surpreende, por um lado, que isso ainda possa ser tema, e, por outro, que tenha passado por transformações em uma velocidade incrível.

1. FERRRAZ JR, Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 88, pp. 439-459, 1993, disponível em: goo.gl/3G2TKQ

Antes de iniciar, gostaria de dizer que esse tema já não é da minha geração: é da nova geração de estudantes de direito. Eu até hoje não consigo lidar com esse vocabulário e esses conceitos com a agilidade com a qual o Juliano consegue, ou, pior ainda, com a qual os filhos dele, que são os meus netos, conseguem.

Recentemente eu li no Estadão um artigo do Fernando Reinach intitulado "Bye Bye Quilograma" que me deixou, não vou dizer triste, mas um tanto quanto perturbado. Ele comenta o fato de que o Metro e o Quilo deixaram de ser um objeto-padrão para se tornar uma relação entre constantes.

> "[O]bjetos padrão são um problema. São mutáveis, podem ser roubados e destruídos e precisam ser copiados para que cada país tenha seu metro e quilo. A solução surgiu quando físicos descobriram que existem certos números, chamados constantes, que são fixos e imutáveis e podem ser usados para definir unidades de medida.
>
> Um dos primeiros atingidos foi o metro. Em 1983, um grupo de cientistas conseguiu medir com precisão uma dessas constantes universais, a velocidade da luz. Ela se propaga a exatos 299.792.458 metros por segundo em todo o universo. Com esse número, foi possível redefinir o metro como a distância percorrida pela luz em 1/299.792.458 segundos (a

definição do segundo é outra história). Com essa nova definição qualquer pessoa pode, com os instrumentos adequados, produzir um metro, em qualquer lugar. E o deus físico da distância, "O Metro", pôde ir do cofre para o museu"[2].

Eu sempre aprendi que o Metro estava depositado em Paris, desde a época napoleônica, como o protótipo de todas as medidas possíveis em metro. Eu me lembro que quando eu era criança a gente tinha em casa uma trena métrica que eu adorava esticar e juntar de novo. Aquilo era um objeto físico realmente. Depois, quando eu aprendi que o Metro existia e que se tratava de uma barra de metal que foi dividida em 100 partes, saber que aquela trena que eu tinha em casa correspondia àquele Metro que estava lá em Paris me deixava emocionado. Agora a emoção se deu às avessas, porque de repente eu descobri que abandonaram isso, aquilo lá vai virar uma peça de museu, e vai ficar uma peça ultrapassada. "Metro" agora é uma relação entre constantes, não tem mais nada a ver com aquele objeto que lá ficou.

2. REINACH, Fernando, "Bye bye quilograma", *O Estado de São Paulo*, 20 de maio de 2017, disponível em: goo.gl/M8RgvZ

Eu comecei a falar disso porque me parece uma referência importante para toda essa discussão. Alguém fazer uma balança que falseia o peso, embora mostre um quilo e tenha menos. Isso me lembra quando eu era levado à feira com a minha mãe quando criança e a gente verificava a balança do feirante. Essa é uma preocupação de muito tempo atrás. Hoje em dia como uma balança que pode ser falseada? Vocês entendem muito melhor os avanços desse tempo e por isso eu me sinto um pouco constrangido em estar desse lado e falar para vocês de um assunto que é de vocês e não meu.

Passada essa rápida observação. Eu gostaria de fazer algumas perguntas que me ocorrem depois de 25 anos de ter es-

crito esse trabalho. Esse trabalho surgiu de uma coisa muito factual em 1991. Eu, naquela época, era procurador geral da Fazenda e enfrentava um problema de revelação do sigilo, de nomes e de dados identificadores de pessoas que portassem cartões de crédito. A primeira vez que enfrentei essa questão me lembro de ter feito uma reunião com grandes empresas de bandeiras de cartões de crédito, porque elas se recusavam a abrir as suas listas de nomes. Aí comecei a refletir sobre o que é que era o sigilo ligado ao uso de um cartão de crédito que é uma coisa absolutamente material – aliás, é até hoje, mas aos poucos vai desaparecer isso – esse cartãozinho que nós carregamos.

Foi por aí que eu comecei a refletir sobre sigilo. Ao refletir sobre esse tipo de sigilo, ocorreu-me também um segundo problema: por conta da Receita Federal, havia uma exigência de que se abrisse aqueles que detinham o cartão, isto é, nomes de pessoas que detinham cartões. Na medida em que as bandeiras diziam "nós não podemos revelar isso", para assegurar que isso não fosse revelado, depositaram as suas listas em banco e com isso garantiram o sigilo via sigilo bancário. Foi todo esse complexo que me levou a refletir sobre sigilo, sigilo de nomes em cartão de crédito, e depois o próprio sigilo bancário, o que é que a gente estava realmente protegendo.

Por conta disso eu fui levado a examinar o art. 5º da Constituição, naquela época já vigente, especialmente o inciso XII, que garante a privacidade e o sigilo, como quase todas as Constituições anteriores:

> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Esse tipo de segredo era uma garantia ligada à correspondência, à telefonia, e, especificamente, à dados: a expressão é "sigilo de dados". Foi isso que nessa época me chamou a atenção e eu quis entender, enfim, o que significavam aqueles dados, sigilo de dados, ao lado da correspondência, ao lado do telefone, e foi por conta disso que eu entrei nesse novo universo. A questão era: o que é que era protegido mediante sigilo conforme dizia a Constituição? O que é que eu estava protegendo?

A Constituição dizia que eu protegia, enfim, correspondência. Naquela época não se usava ainda e-mail. A correspondência para mim era uma carta, algo que vem dentro do envelope e o envelope selado e fechado garantia o sigilo: você não deveria abrir ou rasgar o envelope – era isso que se entendia. Mas também havia um sigilo do telegrama, que era um pouco mais sofisticado, e do telefone, e a Constituição nos dizia que nesses casos eu precisava até de uma autorização judicial para poder entrar nisso. E daí aparecia o sigilo de dados. A minha pergunta era o que é que nós estávamos protegendo ao proteger correspondência, telefonia, telegrafia e a telemática, enfim, o sigilo de dados, o que é que se protegia?

Eu me recordo rapidamente que, ao estudar isso, eu me deparei com comentários sobre decisões da Suprema Corte Americana, em que a discussão girava em torno do objeto da proteção, mediante garantia de sigilo; e o objeto de proteção, segundo essa jurisprudência da Suprema Corte Americana, gerou um debate para saber se o que se protegia era alguma coisa que se via, que se observava, ou se era o direito a essa coisa. A resposta foi, em primeiro lugar, que o que se protegia não era algo, eu não protegia propriamente a correspondência, em termos do papel em que ela transitava, nem o telefone, em termos da voz e tudo mais; o que se protegia, dizia essa jurisprudência, era um direito subjetivo. Sobre isso, existia

também um debate dentro da própria Suprema Corte. Alguns diziam que se tratava de um direito de propriedade, outros diziam que se tratava de um direito à liberdade. A tendência da Suprema Corte foi mais para o lado do direito à liberdade. Então, a proteção do sigilo de correspondência, telegrafia, telefonia e dados seria antes uma proteção à liberdade.

Também me lembro, nessa época, de ter olhado os nossos constitucionalistas. O Pontes de Miranda me deu uma pista que reforçava a tendência nessa direção de que o que se protegia era a liberdade humana. O Pontes de Miranda, comentando a Constituição de 1967 – que falava em sigilo de correspondência e telefonia, mas ainda não em dados, – dizia que o que se protegia era o que ele chamou de liberdade negativa, ou a liberdade de negar informação, o que reforçava a ideia de que o que se protegia era a liberdade e não propriamente propriedade.

Nessa linha, e tentando entender o conjunto o conjunto das situações – correspondência, a telegrafia, a telefonia, a telemática, os dados – já na Constituição de 88, me ocorreu uma distinção, que na época me parecia importante, qual seja a distinção entre os conteúdos de uma informação e a própria comunicação em que essa informação corre, por assim dizer. Isso me parecia alguma coisa importante para merecer reflexão: por eu pensar que eu estava garantindo liberdade com o sigilo, liberdade de quê? Liberdade de corresponder, de telefonar, liberdade de telegrafar – esses verbos aí. Que liberdade, do que é que eu estava falando quando pensava nesse tipo de liberdade? Me pareceu que a palavra – moderna na época – que poderia englobar tudo isso era a chamada *comunicação humana*, e, como havia a possibilidade de eu ligar com a comunicação um objeto desse direito, o direito à liberdade, garantido então pelo sigilo.

Isso me levou a distinguir dois campos que me pareciam diferentes na análise da própria Constituição: de um lado eu

tinha a comunicação, eu imaginava na época uma espécie de fluxo que corria de um para o outro e era isso que se protegia, em termos de sigilo de dados, e isso era direito à liberdade, a liberdade de se comunicar e não ser perturbado por terceiros, era esse fluxo comunicativo que não podia ser atravessado, interceptado etc; de outro lado, isso há 25 anos atrás, 27 na verdade, eu tinha alguma coisa que me parecia que ficava, que restava, e que podia ser então o outro lado da defesa, ou da garantia da liberdade, com garantia de propriedade. Eu percebi que se eu olhasse o outro lado da comunicação, se eu olhasse não propriamente o fluxo e a liberdade de comunicar, mas o meio pelo qual aquilo ocorria, eu tinha alguma coisa que poderia ser visto como direito de propriedade.

Aqui vinham as questões: eu não podia atravessar, interceptar uma correspondência, mas podia apreendê-la, podia apreender a carta, o que restava, era um objeto físico; eu não podia era interceptar, porque o sigilo garantia o fluxo, mas poderia a posteriori requerer que as cartas fossem entregues em juízo etc. O mesmo valia para o telegrama. Aqui me acendia uma luz a respeito da telefonia, porque é que no caso da comunicação telefônica eu precisava da autorização judicial? Naquela época o que me levou à reflexão imediatamente foi o fato de que no telefone o único jeito de você ter acesso era realmente atravessando a conversa, entrando na conversa de dois. Então naquela época eu achava que no caso do telefone era um pouco diferente do caso da correspondência porque a minha ideia era que o telefone não deixava rastros, a não ser que você pudesse gravar. Daí você precisava interceptar o próprio fluxo.

Só que quando eu me deparava com o sigilo de dados, já naquela época, eu sentia que aquilo tinha uma complicação maior ainda. Como é que era possível separar uma coisa da outra? As questões apareciam: os dados bancários de opera-

ções bancárias de alguém são propriedade do banco ou garantem a minha liberdade de realizar operações financeiras? Não se confunde com aquilo que ficava depositado no banco, aquele monte de papel, que hoje praticamente não existe mais. Do que é que nós estávamos falando quando eu lidava com esses dois conceitos: direito de propriedade e direito de liberdade, e olhava para esses dados que não eram mais os que ficaram lá dentro do banco guardados, mas começavam a ser dados trocados mediante esse instrumento novo, que era o da computação?

Hoje repensando essa liberdade negativa da qual nos falava Pontes de Miranda - ou a liberdade de negação como ele dizia - eu acredito que nós estávamos de fato em um mundo que não podia ser carcado, capturado, com aqueles conceitos tradicionais. Uma chave para começar a entender isso me pareceu, já mais recentemente, uma tentativa de refletir um pouquinho sobre aquilo do que a gente estava falando. O que são esses dados dos quais a Constituição falava? A palavra *dado* é uma palavra da língua portuguesa muito anterior a toda essa revolução digital. Mas do que é que eu falava quando pensava nesses outros dados, enfim nesses dados telemáticos, por assim dizer? Qual era o objeto desse tipo de garantia de sigilo?

O que me pareceu algo que merecia a reflexão era entender essa nova forma de a gente lidar com alguma coisa muito antiga que era a noção de informação. O que é que você troca no fluxo de uma comunicação? Nós poderíamos, generalizando, dizer "nós trocamos informações", mas o que é que seriam essas informações quando eu pensava em um mundo digital? Na verdade o que se percebia, e o que se percebe, é que a gente estava diante de algo que não tinha mais propriamente nenhuma materialidade e, para essa ausência de materialidade, eu tinha que identificar na informação alguma coisa nova

para uma expressão completamente nova. A expressão que a gente encontra e é repetida até hoje é "virtual" – é a virtualidade. A gente fala da informação *virtual*, mas o que é que é esse virtual? Palavra portuguesa "virtual" vem do latim *virtus*, que deu virtude, mas obviamente isso não tinha nada a ver com virtude. O que é que era essa virtualidade da informação nesse novo mundo?

Refletindo sobre isso, fui descobrir com um velho amigo meu, um professor tcheco chamado Vilém Flusser que viveu no Brasil e já faleceu, um pequeno artigo sobre esse tema em que ele dava uma pista muito curiosa: ele dizia que isso que nós chamamos de informação nesse sentido virtual não é propriamente algo, alguma coisa, não é – usando a expressão latina – uma *res*. Na verdade não tem nenhuma materialidade, mas também não é propriamente imaterial – não é nem material nem imaterial. À falta de uma expressão melhor, ele dizia, isso que nós chamamos de virtual é uma "não-coisa". Com isso ele queria expressar: olha, não pertence ao mundo com o qual nós estamos acostumados a lidar – mundo atômico, físico – onde eu tenho, por conta de uma antiga tradição, que vem desde os gregos, a possibilidade de perceber materialidades que tomam expressão em vida por conta de formas. Enfim, eu tenho o plástico e de repente ele vira um copo na minha mão, eu tenho a materialidade do plástico e tenho a forma do copo. Esse modo de eu perceber as coisas, diante da virtualidade, foi completamente alterado e transformado. Eu não consigo mais lidar com isso de um ponto de vista da minha percepção do dia-a-dia: como fazer então com a minha percepção do ponto de vista jurídico?

A distinção entre o material e o imaterial é uma distinção que vem desde os romanos e isso é usado largamente. Nós lidamos com objetos materiais e agora com objetos imateriais. Nós temos direitos de propriedade a objetos que são imate-

riais: patentes, etc. Todo esse campo do direito lida com imaterialidades: direito de autor, autoria. Só que quando a gente entra nesse novo mundo telemático, isso não funciona mais; ou seja, toda a forma da gente lidar juridicamente com o nosso mundo que nos cerca e que vinha desde os romanos – e até antes deles – classificando as coisas no mundo como materiais e imateriais, formais e informais, isso não funcionava mais porque eu estava diante de uma não-coisa. Como é que eu lidaria com não-coisas propriamente falando? Isto é, como lidar com certos bens que são não-coisas e que, por assim dizer, não conseguem ser propriamente apropriáveis. Eu não tenho como me apropriar disso.

Do que é que eu estou falando, então, nesse caso? Nós lidamos, por assim dizer, com virtualidade, não-coisas, que dependem de, por assim dizer, um tipo de manipulação muito próxima àquilo que a gente chama de jogo. Nós lidamos com esse mundo, fazendo, ainda, pequenos movimentos com a ponta dos dedos. A mão foi perdendo a sua função. Eu lido com alguma coisa que não consigo mais agarrar. Então, o ser humano como alguém que agarrava as coisas se perdeu. Eu agora trabalho apenas com a ponta dos dedos e, provavelmente, muito brevemente, eu não vou precisar mais nem disso. Por quê? Porque na verdade o que a gente percebe é que nós lidamos com um tipo de objeto que se altera com giros, a gente gira as coisas, e ao fazer esses movimentos você cria mundos, que por assim dizer, estão ali diante dos meus olhos – eu vejo – e ao mesmo tempo são mundos que eu não percebo mais como entrando neles.

Eu me lembro que a primeira vez que eu vi os meus netos brigando, porque um dizia para o outro "eu não quero que você entre no meu mundo", eu não conseguia entender o que eles diziam. Como assim? Entrar no mundo? Eles estavam falando dessa outra situação não *res*, não-coisa, não real, mas

também não informal. E aqui entra de novo a questão do Metro. Não é mais *coisa* nenhuma, é uma pura constante, é uma relação, é uma pura relação.

Nesse caso, aparecem para mim alguns problemas mais complicados: o que é que significa a comunicação que se vale dessa não-coisa, ou que lida com essa não-coisa? No direito penal a gente estava acostumado a falar em busca e apreensão, e busca e apreensão é busca e apreensão de coisas, você busca e apreende coisas. O que é que eu busco e apreendo quando eu lido com essa não-coisa? Eu posso buscar e apreender computadores – isso é uma coisa. Mas não é da *coisa* que realmente estamos falando; mas sim da busca e apreensão relacionada com dados. Aliás, o que menos importa ali é a coisa; o que importa é o conteúdo que está lá dentro e que eu só chego a ele mediante esse neologismo que nós criamos – tivemos que criar – mediante o verbo *acessar*, que não é *ter acesso* no velho sentido. "Acessar" – qualquer criança hoje sabe, eu tenho dificuldade de entender – significa ter a capacidade de movimentar essas constantes na verdade, os tais algoritmos que estão ali, mas que não são nem as coisas que eu vejo e nem aquilo que eu possa imaginar como coisa; são puras constantes que, giradas ou mexidas, fazem com que um livro inteiro surja, um documento, uma petição apareça e que eu possa protestar e dizer que ela não foi conhecida etc. Então, quando eu busco e apreendo esse mundo eu não estou mais lidando com nada referente àquele mundo físico. Portanto acessar os dados muda o perfil jurídico da expressão buscar e apreender. Esse acessar, ainda que eu use a expressão *ter acesso* à, esse *ter acesso* à não tem nada a ver com buscar e apreender, é outro universo, é outra coisa.

Isso mexe com o mundo jurídico? Claro que sim, e não só na busca e apreensão. Recentemente, um caso de direito tributário curioso que me chamou a atenção foi o da venda

de automóvel diretamente da montadora aos clientes[3]. A Lei Ferrari[4] chama isso de "vendas diretas", porque todas as vendas da Lei Ferrari são feitas mediante concessionárias, mas ela admite que você possa fazer vendas diretas. Os exemplos de vendas diretas eram conhecidos: a venda, por exemplo, para uma empresa de locação de automóveis. Você vende diretamente milhares de carros – não um só carro – e nesse caso a montadora pode fazer um acerto direto com o cliente e vender. Como essa é uma venda direta – não tem venda e revenda – isso tem uma implicação tributária óbvia: só tenho uma operação, não tenho duas. Aí eu me lembro que uma das empresas - que me procurou à época, uns 10 anos atrás – resolveu vender carros dentro de uma concessionária, fisicamente falando, mas seu cliente ia lá na concessionária e, usando um computador da concessionária, mediante o programa que estava ali dentro, você conseguia acionar diretamente a montadora. Acionando diretamente a montadora e pondo em contato com o cliente você tinha possível uma venda direta, que não passava pela concessionária.

O fiscal do imposto de renda não entendeu isso de jeito nenhum. Falou: "imagina, isso aqui é fraude, isso não é venda direta; está sendo usada a concessionária, portanto eu tenho venda e revenda, eu tenho dois atos aqui dentro". Esse foi um dos casos que eu comecei a me debruçar e falei "não, isso aqui não é venda mediante concessionária, isto aqui é uma relação direta por telemática". Foi o ano passado que esse caso chegou ao finalmente, com muita dificuldade, no Conselho Administrativo de Recursos Fiscais (CARF). Imagine a discussão que deu para entender o que é que significava vender um carro estabelecendo uma relação direta entre a empre-

3. Ver também FERRAZ JUNIOR, Tercio Sampaio. Lei Ferrari: venda direta pelo fabricante e implicações tributárias. Revista Fórum de Direito Tributário, Belo Horizonte, v. 10, n. 55, jan./fev. 2012. Disponível em: ‹goo.gl/GNNduP›. Acesso em: 3 abr. 2012.

4. Lei Federal nº 6.729, de 28 de novembro de 1978.

/ O QUE É QUE NÓS ESTÁVAMOS PROTEGENDO AO PROTEGER CORRESPONDÊNCIA, TELEFONIA, TELEGRAFIA E A TELEMÁTICA, ENFIM, O SIGILO DE DADOS? /

/ PARECE-ME QUE ESTAMOS DIANTE DE UMA CONCEPÇÃO DE PRIVACIDADE DIFERENTE; ELA ESTÁ MUDANDO. /

sa montadora e o comprador, dentro de uma concessionária e alegando que você não tinha nenhuma revenda. Só nesse novo mundo é que seria possível nós entendermos alguma coisa desse gênero.

Pois bem. Quando a gente se debruça sobre essa nova situação que, por assim dizer, nos perturba em termos de como lidar com os novos mundos que nós fazemos surgir e que aparecem nessas novas situações, surge o tema de como é que eu garanto a inviolabilidade disso. Quando a gente pensava na inviolabilidade da correspondência ou até antes mesmo da casa, encontrava uma ideia da inviolabilidade do sigilo no mundo físico que é muito antiga. Mas aqui surge um tema novo, por quê? Eu percebia essa inviolabilidade no mundo físico, e tinha como lidar com isso. Nós sabíamos que essa inviolabilidade, que podia estar garantida em uma norma constitucional, como está no nosso caso, apontava para situações de fato violáveis. É óbvio que, embora eu garanta a inviolabilidade da casa, a casa pode ser roubada, ou a polícia pode entrar lá dentro, eu posso ter uma ordem judicial; enfim, é perfeitamente possível você quebrar essa inviolabilidade física. Isso pode acontecer também com a correspondência, você manda a correspondência, até para uma penitenciária, e aquilo lá passa por uma revista interior. Você lida com essas inviolabilidades, sabendo que elas podem estar debaixo de uma proteção, mas que a todo momento é possível rompê-las.

E como é que se garantia a inviolabilidade telemática? Bom, aqui surgia essa questão da criptografia. Criptografia não é nada de novo no mundo ocidental, você ter senhas para ter acesso a coisas escritas e a documentos, enfim, você escrever em códigos, isso é uma coisa muito antiga. Mas o problema que nós estamos percebendo hoje, por conta dessa não-coisa com a qual nós trabalhamos sem poder usar com firmeza conceitos como material e imaterial, material e

formal, essa noção da criptografia me parece vai se alterando e ela vai se alterando de tal maneira que é possível – não vou explorar esse caso, vou deixar isso pro Juliano – criar uma tal inviolabilidade que ninguém consegue entrar. Só aquele que detém a senha por assim dizer, ou só aqueles que detêm a senha.

Esse tipo de mensagem trocada, esse tipo de comunicação seria efetivamente inviolável mais do que todo o mundo físico anterior, o que cria um problema sério quando a gente pensa em interesse público e combate à criminalidade, lavagem de dinheiro etc. Como é que eu atravesso isso? É possível nós quebrarmos isso e com base em que, em que direito isso é constituído e como é que eu quebro isso? Bom, eu não vou entrar nessa discussão, o Juliano vai falar disso[5].

5. Ver também FERRAZ JUNIOR, Tercio Sampaio; MARANHÃO, Juliano; FINGER, Marcelo, O desafio do WhatsApp ao Leviatã, Folha de São Paulo, 16 de agosto de 2016, disponível em: goo.gl/L1a6C9

Eu vou falar de um outro lado dessa discussão, pensando agora mais recentemente, como é que está esse sigilo bancário no qual eu pensei estar falando com alguma propriedade há 25 anos atrás. Hoje a gente trabalha com senhas. Vou receber uma ajuda de custo para fazer um exame não doutoramento fora do Brasil e a universidade fora do Brasil para me dar essa ajuda de custo me pediu o meu IBAN. Eu não sabia o que era IBAN e fui atrás para descobrir e percebi que, de fato, cada pessoa, cada cliente do banco, tinha o seu IBAN e eles pediam o meu IBAN. Eu pedi ao banco e o banco falou "eu não forneço". Então como é que eu vou conseguir? "Nós podemos dizer para o senhor, o senhor vem aqui e nós vamos contar para o senhor qual é o seu IBAN". Eu falei "Muito obrigada, tá bom, ótimo". Aí eu recebi e informei a universidade lá fora, aí eles me disseram: "Não, tem que ser em um papel do banco dizendo que esse é o seu IBAN". E agora como é que eu faço? Eu tinha alguma correspondência

do próprio banco e ajeitei a correspondência do banco, um e-mail. Coloquei o IBAN ali dentro e mandei pra eles e eles agradeceram. Enfim, a gente tem que fazer alguma coisa nesse mundo novo, eu fiz desse jeito.

Mas o que é que eu percebo aqui? Aqui começam a aparecer problemas jurídicos complicados e um deles está no exercício de uma profissão antiga nesse terreno bancário que é a profissão de consultor, consultor financeiro, consultor para investimentos. Antigamente, você procurava um gerente do seu banco e perguntava "como é que eu faço investimento?", e isso se faz até hoje. Ele explicava para você "olha, invista aqui, esse aqui está bom". Havia também os consultores privados, gente especializada que você procurava e falava assim "olha, eu tenho dinheiro nesse banco, naquele outro banco, e no outro, o que é que eu faço?", "ah não, tira desse banco, põe no outro, aplica nisso, compre aquilo, tal". Enfim, isso não é uma profissão nova, só que hoje em dia tem um aspecto novo por conta desse novo mundo telemático e nesse mundo telemático você começa a ter esse consultor que pede a alguém a senha, o seu IBAN, e com essa senha ele entra no banco e, ao entrar no banco, ele tem acesso a toda a sua movimentação e ele movimenta. Isso criou da parte dos bancos, aqui do Brasil, um certo desconforto, porque uma coisa é você ter um concorrente que é consultor financeiro e que lida com papeis e que pede a você informações "quanto de dinheiro você tem, em que banco está"; outra coisa é você ceder uma senha para o sujeito e esse sujeito entra dentro da rede do banco e começa a mexer ali dentro.

Aqui surgiu o problema da privacidade e, refletindo sobre essa situação, me pareceu que nós estamos aqui diante de uma concepção de privacidade diferente, ela está mudando. Está bem claro que ela mudou bastante. O *privos* de antigamente era aquilo que ficava dentro de mim ou dentro de um

círculo fechado e dentro desse círculo fechado, imaginando fisicamente o mundo, eu podia entender o que é que significava esse *privos*, a privacidade em oposição àquilo que era público, só que agora nessas circunstâncias eu não consigo mais lidar com isso. O que é a privacidade que se protege nessas circunstâncias? Porque começava a haver uma briga: "de quem é a senha?" "A senha é minha, o IBAN é meu, é só da minha pessoa, só eu como cliente que recebo a minha senha, portanto se a senha é minha e é minha propriedade, mediante do uso da minha liberdade eu dou a senha para quem eu quero". Só que o banco chega e diz "não, a senha é sua, mas a rede é minha, você só pode usar essa senha se você entrar na minha rede e essa rede é o meu sistema, o sistema não é seu"[6].

6. [Nota da editora] Veja, por exemplo, a seguinte disputa entre bancos e o aplicativo GuiaBolso: BRANT, Danielle, "Bradesco trava disputa contra aplicativos que coleta dados de clientes", *Folha de São Paulo*, 28 de novembro de 2016, disponível em: goo.gl/wbk24p

E aqui começou um problema. Ficou mais claro para mim alguma coisa que eu tinha pensado há 25 anos atrás, do que é que nós falamos quando falamos desse novo mundo. Isto é, como é que eu lido com o processo comunicativo aqui? E aqui me ficou razoavelmente claro, que nesse novo mundo, aquilo que nós chamamos privacidade extrapola a ideia do mundo físico antiga - que vem praticamente da revolução francesa, mas até anteriormente - de que liberdade é uma questão de delimitação de espaços. A gente conhece a expressão "a liberdade de um vai até o limite da liberdade do outro". Isso funcionava há uns 230 anos atrás, porque liberdade era estabelecer um espaço: "aqui mando eu e daqui pra frente manda você".

Nesse novo mundo não dá mais para fazer isso: "a senha é minha, mas o sistema é do banco". Se eu começar a jogar com propriedades definindo o direito de liberdades em termos de espaços, eu vou cair nesse problema complicado do chamado

ciberespaço, o *cyberspace*. Isso é uma expressão que começou com um romance na década de 50/60, não foi nenhum técnico que inventou isso. Nesse "espaço", que tem outro sentido, eu não consigo mais traçar uma linha clara para definir o que é o meu e o que é seu. Por quê? Porque eu lido com esse objeto que não é coisa.

Quando eu não consigo mais traçar essa linha fica complicado, por exemplo, como um juiz vai conceder ou deixar de conceder uma liminar garantindo a possibilidade de alguém dar uma senha para um terceiro. Posso dizer que, tendo em vista a sua liberdade e o seu direito de propriedade, aquela senha é dele e ele pode entregar a senha para quem ele quiser? Não propriamente desse modo, porque a senha não é mais apenas aquele número; significa toda uma possibilidade de interação que mexe com um sistema que não é dele e que só faz sentido você ter uma senha dentro desse sistema, onde essa delimitação dos espaços não funciona mais. E se ela não funciona mais, o que é o "meu", o "seu" e o "dele" nesse novo mundo? Como é que eu lido com isso? A interrogação está em aberto, esse tipo de discussão está correndo no nosso tribunal, nos nossos tribunais, de quem é a senha? Dá para eu lidar com propriedade nesses termos?

Bom, o que a gente percebe afinal é que nós estamos, por assim dizer, diante de desafios complicados de nós enfrentarmos e de nós resolvermos e, com isso, estamos precisando provavelmente de um novo instrumental jurídico que ainda não está inteiramente à nossa disposição. O que é que a gente pode pensar a respeito disso? Aqui entram as questões relativas à reflexão sobre essa expressão que ganhou terreno, espaço, no mundo de hoje, que é a noção de transparência. O que é a transparência?

Há 25 anos atrás, não se falava em transparência. Ainda se mencionava o velho princípio da publicidade. Essa era a

palavra forte: "publicidade", que estava ligada ao público em oposição ao privado. Então, havia um direito à publicidade em todos aqueles atos em que havia interesse público e do qual o Estado participava; você tinha direito a que aquilo se tornasse público. A palavra que se usava era princípio da publicidade. Hoje a gente quase que coloca esse princípio da publicidade um pouco baixo, em termos de escala de grandeza, e no lugar disso está entrando essa noção de transparência que é uma noção nova, relativamente, do ponto de vista jurídico. A exigência de transparência não é propriamente a exigência de publicidade, pois o que precisa ser controlado é outra coisa. Aqui surge uma dificuldade: como é que eu lido com revelações que tem que ser então tornadas públicas, principalmente nesse tipo de mundo que é o mundo telemático? Nós tivemos um exemplo recente, o Ministro Edson Fachin liberou uma gravação – fruto de uma interceptação – no âmbito de uma delação premiada e pegou um jornalista que não tinha nada que ver com isso. Ele acabou pedindo demissão. Atingiu a vida dele, como é que você lida com um negócio desse? O que é que significa publicidade dentro desse mundo da transparência? A exigência de transparência é uma exigência nova. Ela está ligada a essa repercussão que tem esse universo telemático no mundo que nós vivemos; não é mais a publicidade. Transparência é outra coisa e que está deixando a gente bastante aflito, para dizer o mínimo. O que é que era o princípio da publicidade?

Eu me lembro de um trabalho, do Niklas Luhmann, um sociólogo, escrito em 1969[7], há muito tempo, em que ele dizia que o princípio da publicidade no direito tinha uma função: aquietar a curiosidade pública, não transformar dados, quais fossem naquela época, em dados públicos, mas aquietar a curiosidade pública. Então, a porta

7. Ver LUHMANN, Niklas. *Legitimation durch Verfahren*. Frankfurt a.M.: Suhrkamp, 1969

tinha que ficar aberta, sendo uma cerimônia oficial, porque ela era pública, não para que todo mundo entrasse, mas para que todo mundo pudesse entrar. Porque na medida em que ficava aberta, ninguém entrava, ou entrava um. Quem é que vai a um tribunal aqui em São Paulo e olha, vê o juiz sentado lá com duas partes e fala "dá licença, eu quero assistir"? Ninguém faz isso. Mas é público, está coberto pelo princípio da publicidade. Como é que ele funciona? Ele funciona dizendo que está aberto para quem quer que chegue. O princípio da publicidade legitimava certas situações, nesse sentido.

A transparência é outra coisa. A transparência cria problemas percebidos pelo Luhmann à sua época. Dizia o Luhmann que se nós transformarmos o princípio da publicidade em algo empiricamente exigível – que todo mundo entre em todas as salas, – você vai arrebentar com o princípio, ele não vai funcionar mais, você vai esgotá-lo. Ao esgotá-lo, ele vai perder sua função, nada vai ser mais legítimo, porque tudo é visível e tudo é uma, enfim, não pode ser desse jeito.

No mundo da transparência, nesse mundo que nós estamos vivendo, nesse mundo da telemática, isso não só é possível como está acontecendo. Então, todos queremos ver tudo, inclusive os ministros discutindo e brigando uns com os outros no Supremo Tribunal Federal. Isso não é publicidade, isso é transparência. Essa transparência acaba provocando efeitos novos e surpresas enormes, reações que antigamente você não tinha, ninguém percebia. Quem é que tinha pachorra e paciência de ouvir ministro do Supremo discutindo? Ninguém fazia isso. Vá lá sobre o princípio da publicidade. Agora vira novelinha da Globo, está todo mundo ali em cima assistindo. Isto é, a transparência está criando um outro mundo e como é que essa transparência entra dentro do nosso mundo telemático? Enfim, aqui é que as questões começam a ser colocadas talvez de uma forma nova.

Como nesse mundo telemático a gente tem que usar, a gente tem que perceber que o que está em jogo não é o "meu" e o "seu", isto é, eu não lido mais com esse espaço; nesse mundo da transparência nós temos que começar a repensar a publicidade em termos de princípios que garantam a identificação, a identificação de quem está ali dentro, a identificação dos parceiros. Isso é que tem que começar a ser transparente, seja uma comunicação pública, ou seja ela privada. Seria preciso nós ordenarmos isso juridicamente, isto é, repensar o anonimato, repensar situações como essas dentro de um sistema bastante peculiar, por assim dizer. As regras que nós temos, portanto, que observar devem obedecer a situações novas onde a distinção entre uma e outra posição não é mais clara em termos espaciais.

Bom, por fim, o que é que a gente pode pensar a respeito dessa nova situação quando nós lidamos com normas do tipo: "constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou objetivos não autorizados em lei"? Isso é um artigo de lei, art. 10 da Lei 9.296/1996. Como é que a gente imagina esse crime de interceptação? Quando a gente pensava nas comunicações telefônicas, ou em quebrar um segredo de justiça, dava para gente imaginar com razoável precisão o que é que significava essa interceptação. Nesse nosso novo mundo, onde o acesso é que conta, isso obviamente é, do ponto de vista jurídico, muito mais complicado de nós imaginarmos e de nós trabalharmos, por assim dizer. Nessa situação, nós imaginarmos que a interceptação de comunicações telefônicas, para investigação criminal ou para instrução processual, terá que, como diz o §único do art. 1º dessa própria lei, "o disposto nessa lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática". Confesso que o caput do artigo "interceptação

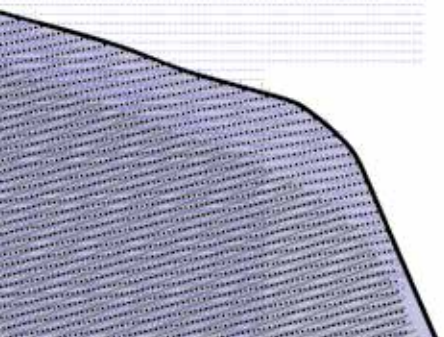
de comunicações telefônicas de qualquer natureza para prova, investigação criminal, ou instrução processual penal" é para mim razoavelmente claro. Mas o §único é extremamente complicado; nós estamos falando de coisas completamente diferentes. Em outras palavras, lidar com a lei, ou com os dispositivos legais, nesse novo mundo é muito mais difícil do que eu possa imaginar.

Um ex-aluno meu me perguntou o que eu aconselharia a um juiz diante de normas como essa. Eu falei que não sei o que é que eu diria para um juiz, mas que você tem dois problemas sérios hoje. Antigamente os juízes abordavam a legislação mediante um instrumento que mediava o seu acesso às normas da legislação e que se chamava doutrina. Hoje, no Brasil, isso está desaparecendo. A doutrina não conta mais; ao contrário, para alguém que quer saber o que é que diz uma lei, um artigo de lei, você olha a jurisprudência diretamente, você quer saber o que os tribunais disseram. E nessa situação, desse mundo telemático, em que eu não tenho doutrina, e estou jogando tudo para o juiz, a posição dos juízes é terrivelmente complicada, eu diria que é de uma brutal angústia: você continua lidando com doutrinas antigas no mundo físico e lidando com situações como se elas pudessem ser resolvidas desse modo. Eu tenho a impressão que isso é de fato apenas uma fachada, muita coisa se perde nessa relação.

02.

O QUE É DADO NÃO É COMUNICADO?

Juliano Maranhão



Transcrição da palestra feita por Heloísa Massaro. Editado por Jacqueline de Souza Abreu. Revisado por Juliano Maranhão.

Já que o professor Tércio abriu aqui a nossa vida privada, eu vou trazer um outro episódio que também é muito curioso com relação aos netos dele, que são meus filhos. Um dia, eu liguei para o meu mais velho, porque eu queria passar em casa para pegá-los e levar os dois para o clube. O mais velho atendeu o telefone e eu perguntei: "o Danilo está com você?", e ele falou "está" e fui para casa pensando que ia pegar os dois. Cheguei lá e estava só o Emiliano, o mais velho; o mais novo estava na casa do avô, estava com a avó. Eu perguntei "mas vocês não estavam juntos?" "Estávamos, no Minecraft". Ou seja, o significado de estar junto para eles é bastante diferente do nosso. E esse exemplo também que eu presenciei do choro do mais novo porque ele não podia entrar no mundo, mostra que para eles, na linguagem, na concepção deles, que crescem nesse ambiente virtual com uma naturalidade muito maior, o mundo virtual tem um sentido de existência que para nós é inconcebível. Essa percepção da mudança na linguagem natural, quando você conversa com as crianças, é ilustrativa. É interessante para perceber de que forma a linguagem molda e reconstrói, constrói realidades.

Isso é particularmente verdade dentro do direito. Afinal de contas, aqueles que se dedicam ao direito estão mais acostumados a lidar pelo menos com uma "realidade virtual" que é o "mundo jurídico". Quem estuda o Kelsen conhece a diferença entre o *dever ser* e o *ser*, o mundo dos fatos e o mundo jurídico. Isso é uma metáfora interessante e, no mundo jurídico, é possível fazer uma série de coisas que no mundo dos fatos nós não podemos. Por exemplo, é possível viajar no tempo: o Supremo Tribunal Federal vive fazendo isso, mexe em relações jurídicas passadas e molda essas relações para o futuro, com a modulação dos efeitos da sentença, coisas que estão fora do alcance da física (pelo menos atual). Justamente para se proteger desses poderes especiais que nós temos, no

mundo jurídico, outros conceitos – como "irretroatividade" e "direito adquirido" – para lidar com essa forma pela qual nós falamos sobre o tempo no mundo jurídico, que é diferente da forma pela qual nós falamos sobre o tempo no mundo real.

O tema que foi trazido para a discussão aqui também envolve uma indefinição com relação a certos conceitos que são importantes, que são centrais, e que vão definir a forma pela qual os tribunais ou os juristas entendem o que são dados, o que é comunicação. Existe uma distinção importante e inicial aqui que aparece entre dado como uma espécie de objeto – o professor colocou bem a dificuldade em lidar com um objeto que não é real, é virtual; e, por outro lado, a comunicação como um processo. Outro aspecto interessante é que os tribunais vivem na angústia de ter que lidar com esses conceitos a partir daquilo que é palpável e daquilo que experimentaram no mundo físico, e as analogias aparecem por aí.

Nessa discussão, em particular, sobre busca e apreensão, acesso a dados, o grande alvo das investigações são as trocas de mensagens no WhatsApp. Há duas analogias aqui que são básicas. Uma delas é aquela que busca comparar e aproximar o dado - que é na verdade é um dado virtual, um objeto -, a uma carta. Fazem analogia com a carta, que pode se encontrar em um domicílio, ao passo que o correspondente analógico mais próximo à ideia de processo de comunicação é a ligação telefônica. Essas duas figuras, esses dois parâmetros, não bastam para dar conta dos meandros tecnológicos e os tribunais enfrentam dificuldades com relação a isso. Eu trouxe algumas dificuldades aqui para colocar na mesa, para depois nós discutirmos.

Essa ambiguidade está presente tanto no Supremo Tribunal Federal (STF), quanto está presente no Superior Tribunal de Justiça (STJ), que são os principais tribunais de interpretação e uniformização de jurisprudência. No STF, em breve vai ocorrer a audiência pública para discutir o tema do bloqueio

do WhatsApp[1]. O bloqueio se dá em função de uma regra que permite a suspensão das atividades da empresa, no caso do WhatsApp, quando há recusa em cumprir uma ordem judicial de interceptação telefônica. Portanto a discussão no STF que está em aberto hoje é o WhatsApp encarado como uma espécie de comunicação, e o que se discute é se a interceptação pode ou não pode ser feita e se posso suspendê-la em função da interceptação dessa comunicação.

1. A audiência pública ocorreu nos dias 2 e 5 de junho de 2017. Mais informações podem ser encontradas em: Abreu, Jacqueline de Souza. "Audiência Pública sobre Criptografia e Bloqueios do WhatsApp: argumentos diante do STF", in: bloqueios.info, InternetLab, 26 de junho de 2017, disponível em goo.gl/TPme2Z

Por outro lado, no próprio STF há um caso, cujo relator foi o Gilmar Mendes, em que houve uma apreensão de um aparelho celular em 2004, quando o aparelho não tinha tantas funcionalidades como agora[2]. Nesse flagrante foram utilizados determinados dados que estavam registrados, registros de telefonemas, e ali apareceu, pelo Gilmar Mendes, uma analogia interessante, ligada a essa metáfora da carta. Gilmar Mendes disse: "*indago: e se o número estivesse em um pedaço de papel no bolso da camisa usada pelo réu no dia do crime, seria ilícito o acesso pela autoridade policial? E se o número estivesse anotado nas antigas agendas de papel ou em um caderno no momento da prisão?*" Esse é um momento do voto em que ele mostra grande convicção; percebe-se que é um momento da construção retórica em que o Ministro se convence efetivamente de que a situação é a mesma de um papel; eu não teria o menor problema de utilizar um papel no bolso – o dado, o número de telefone no aparelho celular, seria exatamente a mesma coisa.

2. SUPREMO TRIBUNAL FEDERAL. Segunda Turma. Habeas Corpus 91.867-Pará. Min. rel. Gilmar Mendes, julg. 24 de abril de 2012.

Então há, no STF, esses dois momentos em que, de um lado, um dado é considerado um objeto, semelhante a um objeto físico, um papel; e, de outro lado, uma comunicação.

No STJ também há dois casos interessantes. Há o Habeas Corpus de 2016, que foi relatado pelo Ministro Nefi Cordeiro, em que se tratava também de uma prisão em flagrante[3]. Naquele caso, o Ministro não autorizou o uso dos dados; ele neutralizou o uso que foi feito, por não existir um mandado judicial de interceptação telefônica. Considerou-se que não se deveria ter acesso a mensagens de WhatsApp porque aquilo era uma comunicação. É interessante que naquele caso houve voto-vista do Ministro Rogério Schetti, em que ele faz menção a um caso da Suprema Corte norte-americana, que é o *Riley vs. California* de 2010, para discutir justamente aquele precedente do STF do Gilmar Mendes de 2004, julgado em 2012. No fundo ele considera que aquela mensagem do WhatsApp não é propriamente comunicação, é dado, mas diferentemente daquela decisão de 2004, ou seja, 10 anos depois, considera que o celular evoluiu, não é simplesmente um aparelho para realização de comunicações e, portanto, ele reúne todos os dados íntimos da vida – quase que considera o celular uma espécie de domicílio. Conclui que seria necessário ter mandado específico para acessar aqueles dados.

3. SUPERIOR TRIBUNAL DE JUSTIÇA. Recurso Ordinário em Habeas Corpus nº 51.531/RO. Min. rel. Nefi Cordeiro. 6ª Turma, julg. 19 de abril de 2016.

Estive com o Ministro Schetti em uma conferência na semana passada, quando perguntei a ele: mas o mandado seria aqui de interceptação telefônica ou de busca e apreensão? Porque essa ambiguidade não está resolvida. E depois, num caso mais recente de 2016, em que se tinha uma busca e apreensão de celular, o STJ, em um voto do Ministro Felix Fischer[4], admitiu que os dados fossem acessados e, para fundamentar essa decisão, utilizou a distinção que foi cunhada no artigo "Sigilo de dados: o direito à privacidade e os limites à função

4. SUPERIOR TRIBUNAL DE JUSTIÇA. Recurso Ordinário em Habeas Corpus nº 75.800/PR. Min. rel. Felix Fischer. 5ª Turma, julg. 15 de setembro de 2016.

fiscalizadora do Estado"[5] do professor Tércio, que ele acabou de trazer, e ali ele diz claramente "*a proteção da lei de interceptação se refere ao fluxo das comunicações de sistemas de informática e telemática, a proteção é do curso da conversa desenvolvida pelos interlocutores, não há, portanto, vedação ao conhecimento do conteúdo dessa interação quando ela já se encontra armazenada*". Aqui é "dado", portanto, um objeto que pode ser apreendido, como uma carta que poderia ter sido encontrada na residência em que foi feita a busca e apreensão. Conclui que não haveria necessidade de mandado específico para acessar essas informações.

5. FERRRAZ JR, Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, pp. 439-459, 1993, disponível em: goo.gl/cojEJc

Com relação a essa metáfora ou a essa analogia com a carta, o Tribunal Constitucional Alemão tem um caso que é um divisor de águas. Trata-se do caso *Handy-Verbingunsdaten*, que lidou com acesso a registros de conexão que estavam em um celular que foi apreendido.[6] O Tribunal fez de novo essa distinção entre "comunicação", de um lado, e "dado", do outro, e disse com todas as letras: não há razão para tratar os dados armazenados em um celular diferentemente de uma carta encontrada em um domicílio; aquilo é dado, aquilo é objeto, a carta poderia ser destruída assim como os dados poderiam ter sido apagados. Essa foi a fundamentação. Tem uma pequena diferença, porque na Alemanha existe, de um lado, o sigilo das comunicações, que é protegido pela Constituição, e existe também a proteção de dados, em nome da autodeterminação informacional, que é outra esfera de proteção reconhecida pela corte constitucional. Então, de uma certa forma, a privacidade não fica desguarnecida como no nosso caso em que nós não temos ainda uma boa definição sobre proteção de dados.

6. BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 04. Februar 2005 - 2 BvR 308/04 - Rn. (1-29), goo.gl/LDi1w2

/ NÃO SEI SE A ANALOGIA COM UMA CARTA, QUE PODE SER RASGADA, FAZ SENTIDO QUANDO SE TRATA DE UMA COMUNICAÇÃO COM O CELULAR [...] /

/ A FUNDAMENTAÇÃO QUE ESTÁ POR TRÁS DA PROTEÇÃO DO SIGILO DE COMUNICAÇÕES TEM A VER COM A PROTEÇÃO DE UMA LIBERDADE EM SE COMUNICAR. /

Mas o que é interessante discutir aqui? Essa analogia com a carta tem problemas: de um lado, uma carta, que eu posso destruir, de outro, uma comunicação, em que os dados se armazenam. Isso não é tão simples. Para começar, a carta se duplica. Em segundo lugar, boa parte da fundamentação que se atribui ao caso da carta encontrada e o tratamento do celular como se fosse um dado apreendido está na ideia de que aquele dado esta no domínio do usuário e que ele poderia ter destruído na busca e apreensão. Eu não sei se essa analogia com a carta, que pode ser simplesmente rasgada, pode ser feita quando se trata de uma comunicação com o aparelho celular, que tem uma série de registros e dados que ficam armazenados e que nem sempre o usuário comum, para começar, sabe que aqueles dados, aqueles registros são feitos, muito menos apagá-los.

Algo mais importante diz respeito ao próprio objeto de proteção. A fundamentação que está por trás da proteção do sigilo de comunicações tem a ver com a garantia da confiança no sistema de comunicação. É por meio dessa garantia de confiança que se protege a liberdade, a liberdade em se comunicar. Ou seja, é como se o direito construísse um simulacro em que a comunicação à distância seria equivalente a uma comunicação entre presentes, longe do olhar de todos e é a confiança nesse simulacro o que se discute. Na medida em que eu tenho um sistema confiável, eu sou livre para me comunicar e o que se protege no final das contas aqui é a liberdade de pensamento, isto é, eu poder expressar aquilo que eu penso nessa comunicação sem nenhum constrangimento, sem me sentir intimidado com a possibilidade de que aquele conteúdo seja conhecido por um terceiro. É privacidade, mas de uma certa forma é também uma proteção à liberdade de expressão. Quando eu penso em dado isso não está presente, aí é bem diferente.

Agora, quando a gente pensa no WhatsApp, tem uma coisa muito interessante quando nós tentamos fazer essa analogia

com esses dois elementos que são as referências usadas: de um lado, ligação telefônica, e, do outro lado, a carta, no domínio daquele que é apreendido. Isso tem a ver com como é que a gente deve interpretar a tal "comunicação em curso", o fluxo da comunicação, porque quando nós pensamentos na comunicação telefônica, esse curso de comunicação vale para dois aspectos: tanto o fluxo da comunicação, da transmissão dos dados, começa e se interrompe durante aquela ligação telefônica; e a conversa também, o curso da conversação começa e termina exatamente no mesmo momento daquele fluxo da transmissão do dado; então fluxo do dado e o período de conversa coincidem quando a gente fala numa ligação telefônica. Mas agora no WhatsApp? No WhatsApp a noção de tempo é diferente da noção de espaço que nós estamos acostumados – assim como a noção de espaço para meus filhos é diferente da minha. O WhatsApp traz outra noção de tempo de transcurso da conversa: de um lado o fluxo da comunicação é momentâneo em diversas mensagens, mas, em termos do curso da conversa, nós não sabemos muito bem quando uma conversa pelo WhatsApp termina: posso responder imediatamente, posso esperar, posso responder depois, posso responder no dia seguinte, e a conversa ainda não terminou.

Essa distinção é importante, porque se nós pensarmos que o objeto de proteção aqui é, na verdade, o não constrangimento dessa liberdade em se comunicar, talvez o relevante não seja propriamente o tempo de transmissão, mas seja propriamente a espontaneidade ou a liberdade em expressar pensamento no curso de uma conversação. Se isso for verdade, fica mais difícil diferenciar dado armazenado, como algo fixo que pode ser apreendido. Você passa a olhar aquelas mensagens trocadas no WhatsApp como uma comunicação em curso – não o fluxo de transmissão de informação, mas uma conversa ainda em ação.

Bom, eu trouxe esses temas mais para abrir para uma discussão e queria ouvir também o professor um pouco mais sobre isso.

< TÉRCIO SAMPAIO > Eu já falei bastante. Eu apenas comentaria dizendo que uma ideia que é recorrente nos tribunais é buscar analogias; parece que você só consegue lidar com essas situações tentando fazer analogias, que, como toda analogia, pode ser mais ou menos perfeita. No caso, de fato é bastante difícil. Acho que, eu próprio, quando escrevi há 25 anos atrás o artigo e joguei com a noção de fluxo comunicacional e o resultado da comunicação, estava pensando na correspondência; eu estava pensando na telegrafia, ainda entrava; no telefone eu já sentia que era mais difícil. Eu sabia naquela época que você tinha, junto com a proteção ao sigilo telefônico, a proteção também à sua conta telefônica. Como Procurador Geral da Fazenda, eu lidava com isso, quer dizer, você protegia não apenas o telefonema, mas também o registro de quem você chamou. Quer dizer, a sua conta telefônica, além da conversa telefônica, ela é protegida pelo sigilo. Agora, em tudo isso dá para você lidar com a noção de fluxo comunicacional e o resultado da comunicação.

Eu reconheço que a dificuldade, que na minha época não me parecia tão difícil assim, está em você lidar com a comunicação telemática, vamos chamar assim, em termos de separar o *fluxo* do *resultado*. Eu reconheço, é muito difícil fazer isso, tecnicamente falando. Agora, na cabeça de quem estudou direito dentro do outro mundo, as soluções acabam sendo desse jeito, só que elas acabam, por assim dizer, saindo um pouco pela tangente, porque você não consegue, diferentemente de outras situações, lidar com essa separação de uma maneira clara.

O exemplo da armazenagem poderia dar uma certa força à analogia: aquilo que você armazena é, para assim dizer, o resultado da comunicação; o fluxo é diferente dessa armaze-

nagem. Só que essa armazenagem, ao contrário do mundo físico, não é algo que esta ali e que é diferente do próprio fluxo, esse é o problema. Ou seja, a ideia de original e cópia, nesse mundo, não funciona mais desse jeito, você não tem mais o autêntico e depois a cópia, a cópia em termos informáticos é absolutamente inseparável do "original", o que talvez nos dê essa medida de dificuldade entre você separar o fluxo da própria armazenagem. Quer dizer, no fundo é a mesma coisa e só com um artifício, na hora de tomar a decisão, é que você olha para o celular e diz "é como se fosse um caderninho de notas". Não é um caderninho de notas, é completamente diferente.

Por enquanto a gente trata desse jeito, só que quando você trata desse jeito, você acaba interferindo em inviolabilidades que antes você conseguia separar. No seu caderninho de notas provavelmente você não teria a possibilidade de cometer uma incursão na vida de terceiros como aconteceu em tornar pública uma delação premiada desse jeito. Ela não está mais em um registro policial, papel etc., ela está em outro registro e ali a dificuldade está em como é que você protege as diferentes individualidades? E por falar em individualidade, esse é um outro problema.

Essa situação nova está criando um tipo de personalidade diferente. O que é que é hoje uma pessoa? No velho sentido jurídico, a defesa da pessoa humana, direitos fundamentais, o que é que é essa pessoa quando você se comunica por meio telemático, o que é que é essa pessoa? Eu sou identificável, na verdade, por um número de IBAN, eu não sou uma pessoa no outro sentido, no velho sentido; na verdade eu sou apenas um número. Parece que o progresso, brevemente no Brasil, vai nos levar a essa carteira de identidade que não é mais nem esse papel, nem esse bilhete que a gente carrega no bolso, mas vai juntar todos os meus dados – uma coisa terrível, a exposição por assim dizer é total. Com a minha identidade eu estou completamente revelado. A possibilidade de você

dizer “o que não está nos autos não está no mundo” acabou. A hora que eu entro nos autos e dou a minha identidade está toda a minha vida ali dentro. Como é que eu separo isso? Eu acho que esse é o desafio para uma jurisprudência e para uma doutrina tentarem inventar: vai ter que inventar uma outra noção de pessoa, muito diferente da pessoa que surgiu lá com os gregos, a máscara que cobria o rosto do que morria. Vai realmente acabar isso. Vamos ter ainda bastante espaço para discussões como essa.

< JULIANO MARANHÃO > O professor Tércio está um pouco pessimista com relação ao futuro da doutrina, mas, de fato, diante do volume de ativismo dos juízes, a academia fica até um pouco encolhida, mas com certeza a atitude correta não é transformar a academia em meros relatores de decisões judiciais. Eu acho que essa construção conceitual precisa acontecer na academia. A ideia de proteção de dados, aliás, foi algo que apareceu primeiro na academia para depois ter um reconhecimento pelo Tribunal Constitucional Alemão. A ideia do direito fundamental, a autodeterminação informacional, que é uma construção muito importante e começa a ser mencionada aqui no Brasil pelos tribunais, é algo que apareceu na década de 70 na universidade de Frankfurt, em particular, com uma construção interpretativa da Constituição, e que depois foi ganhar em 83 o reconhecimento pelo Tribunal Constitucional. Na Alemanha, se você perguntar em uma biblioteca sobre direito e internet, não encontrará muitos livros sobre isso. Mas se você pergunta sobre *Datenschutz*, encontrará bibliotecas inteiras. Então, toda a construção doutrinária se deu em cima de proteção de dados que é um pouco o que está acontecendo às avessas aqui. Falar em direito e internet, uma série de princípios, de transparência, etc., sigilo, mais genéricos, mas ainda falta um documento de proteção de dados. Há uma grande lacuna ainda na nossa legislação.

03.

SMARTPHONES: BAÚS DO TESOURO DA LAVA JATO

Dennys Antonialli, Francisco Brito Cruz e Mariana Giorgetti Valente

Texto originalmente publicado no blog Deu Nos Autos, do Link Estadão, em 24 de novembro de 2016.

As práticas de investigação criminal da Operação Lava Jato têm levantado debates jurídicos acirrados: em delações premiadas, prisões preventivas, cooperação internacional, o Judiciário vem dando acolhida a novas interpretações propostas pela Polícia Federal e pelo Ministério Público (as chamadas "forças-tarefa") na repressão a crimes de colarinho branco. Junto com os ganhos da Operação, surgem questionamentos a respeito das práticas adotadas, por vezes denunciadas como interpretações muito "extensivas" da legislação, a violar os direitos de defesa dos acusados. Parte da comunidade jurídica preocupa-se, especialmente, com a consolidação dessas interpretações por tribunais superiores – o Supremo Tribunal Federal (STF) e o Superior Tribunal de Justiça (STJ), de forma a cristalizá-las.

Nessas operações, as "informações digitais" assumiram um papel central. Afinal, a vida conectada deixa muitos rastros: você já parou para pensar em quantas informações estão armazenadas só nos telefones celulares? São agendas de contatos, arquivos de textos, fotografias tiradas diariamente, anotações, caixas de e-mails, históricos de mensagens instantâneas, históricos de navegação na Internet, informações de GPS sobre cada lugar que visitamos e que caminho fizemos. Resumindo: nossos smartphones se tornaram verdadeiros "baús do tesouro" para investigadores.

Se é evidente que essa grande disponibilidade de informações pode facilitar uma investigação judicial, também cresce a possibilidade de acesso pelas autoridades a muito mais informações do que seria necessário e razoável, o que levanta preocupações sobre privacidade, intimidade e outros direitos, como liberdade de expressão e de associação. É razoável que uma equipe de investigação tenha, por exemplo, acesso à sua caixa de e-mails inteira, para descobrir algo sobre uma comunicação específica entre você e um potencial infrator? O que está em jogo, no fim das contas, é uma questão democrática importantíssima: quais os limites que

devem ser impostos ao Estado em relação aos direitos e liberdades individuais das pessoas, ainda que o combate à corrupção e a outros crimes seja também um objetivo a ser alcançado?

O próprio início da Lava Jato esteve marcado por controvérsias desse tipo: em 2014, o acesso a mensagens trocadas por um dos réus, Alberto Youssef, foi o elemento-chave para a força-tarefa recolher elementos sobre o esquema de propinas operado – e depois delatado – por ele. A forma como a operação obteve acesso às mensagens foi questionada pela defesa:[1] ela teria infringido os procedimentos formais existentes de cooperação internacional ao pedir *diretamente* para a matriz estrangeira da empresa fabricante dos telefones (RiM, que fabricara os *Blackberries* dos investigados) o conteúdo das conversas.

1. CANÁRIO, Pedro. Relação direta entre PF e empresa canadense alarma advogados da "lava jato". Consultor Jurídico, 10 de novembro de 2015. Disponível em: goo.gl/HyZRsy

O STJ acaba de decidir, como tem feito em muitos outros casos, sobre uma questão controversa como essa. Desta vez, a defesa de um dos réus da operação alegou que o juiz Sérgio Moro não poderia ter aceito como prova *conversas armazenadas* em um smartphone apreendido em cumprimento a uma de suas ordens de busca e apreensão. Ou seja, o simples fato de se ter apreendido o aparelho mediante ordem judicial (de busca e apreensão) seria suficiente para garantir o acesso a tudo que existe dentro dele (incluindo as conversas), sem necessidade de uma outra ordem judicial, específica para isso.

Para o STJ, Moro agiu corretamente. De acordo com a decisão, como não se trata de uma *interceptação de comunicações*, que exigiria o cumprimento de requisitos mais estritos de autorização judicial (como determina a Lei n. 9.296/1996), não haveria necessidade de obtenção de nova ordem específica. A decisão vai na linha do que o STF também já decidiu[2] em relação ao acesso a emails

2. SUPREMO TRIBUNAL FEDERAL. Recurso Extraordinário n. 418.416-8 SC. Min. Rel. Sepúlveda Pertence. Julg. 10 maio 2006. Disponível em: goo.gl/58Ni4w

armazenados em computadores apreendidos pela polícia, conforme apontamos no relatório do InternetLab sobre vigilância das comunicações no Brasil[3].

É verdade que, em sua ordem de busca e apreensão, Moro conferiu plenos poderes de acesso à polícia: "(...) *poderão as autoridades acessar dados armazenados em eventuais computadores, arquivos eletrônicos de qualquer natureza, inclusive smartphones, que forem encontrados* (...)". Contudo, essa autorização genérica e irrestrita a quaisquer informações armazenadas precisa ser colocada em perspectiva.

A argumentação do STJ parece estar calcada na seguinte premissa: a legislação confere uma proteção maior ao *fluxo das comunicações* do que às informações armazenadas. Isso significa que é muito mais difícil conseguir autorização para interceptar uma ligação ou um endereço de email do que para ter acesso ao que está guardado em um smartphone.

No passado, isso parecia fazer sentido: os celulares eram enormes "tijolos" que apenas faziam e recebiam chamadas. Grampear uma ligação era uma das únicas maneiras de se ter acesso a uma série de evidências e, portanto, umas das maiores violações à privacidade que se poderia cometer. Foi nesse contexto que a Lei de Interceptações foi pensada, em 1996. Hoje, essa realidade se inverteu. A legislação, no entanto, não acompanhou, de forma que esses tesouros de dados ficaram sem proteção.

Vejam como estamos lidando com um descompasso: essa interpretação sobre os *dados armazenados*, que é compartilhada pelo juiz Sérgio Moro, pelo STJ e pelo STF, vem se baseando, por exemplo, em um texto escrito em 1992 por um importante jurista, o prof. Tercio Sampaio Ferraz Jr. Para ele, eventuais quebras de sigilo "de dados" (o exemplo dado no texto é o do acesso a extratos bancários) não violariam a Constituição, por não serem "grampos" (que pela Constituição são permiti-

3. Referência a ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017, pp. 41-45. Disponível em: goo.gl/TQ7U8E.

/ NO AFÃ DA CONVULSÃO POLÍTICA PELA QUAL PASSA O PAÍS, SOLIDIFICAM-SE ENTENDIMENTOS QUE PODEM COMPROMETER DIREITOS DE TODOS NÓS. /

/ É MUITO MAIS DIFÍCIL CONSEGUIR AUTORIZAÇÃO PARA INTERCEPTAR UMA LIGAÇÃO DO QUE PARA ACESSAR O QUE ESTÁ GUARDADO EM UM SMARTPHONE. /

dos apenas em casos excepcionais). Quase vinte e cinco anos depois, vale a pena questionar se não estaríamos utilizando parâmetros jurídicos arcaicos para lidar com novíssimas formas de comunicações. O que é mais privado: tudo o que está salvo no seu celular, o que pode incluir vinte anos de e-mails, ou o conteúdo de uma ligação que você realiza?

Ainda que o enquadramento que a decisão oferece esteja correto – o caso em questão não trata de uma interceptação de comunicações propriamente -, com nossos celulares sendo repositórios de tantas informações, seria essencial o estabelecimento de limites em relação a quanto e quando se pode ter acesso ao que está guardado dentro deles. Nos Estados Unidos, como já comentamos aqui[4], essa questão já foi enfrentada pela Suprema Corte, que, por unanimidade, decidiu ser necessária uma *ordem judicial específica* para o acesso a dados armazenados em um aparelho celular, mesmo que ele já esteja em poder da polícia depois de uma busca e apreensão (caso *Riley v. California*).

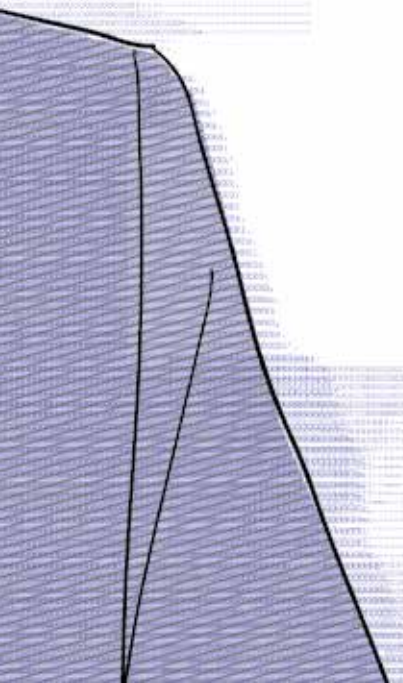
4. ANTONIALLI, Dennys; CRUZ, Francisco Brito; VALENTE, Mariana Giorgetti. Você tem o direito de manter seu celular calado? *Deu nos Autos*, 1 out. 2015. Disponível em: goo.gl/tRZBo6

Além do sigilo das comunicações (art. 5, XII), a Constituição Federal também determina a proteção do direito à privacidade (art. 5, X), o que deve ser levado em consideração em decisões como essa. Em vez de ser vista como escudo para potenciais criminosos, a privacidade também precisa ser encarada como um dos pilares do estado democrático de direito, sem a qual ficam ameaçados o livre desenvolvimento da personalidade e o exercício das liberdades civis.

Se a Lava Jato vem produzindo imensos impactos na investigação criminal e em uma série de processos sociais, também quanto aos *direitos digitais* ela precisa ser acompanhada de perto e submetida à crítica. No afã da convulsão política pela qual passa o país, solidificam-se entendimentos e práticas que podem comprometer direitos de todos nós.

04.

A PRISÃO EM FLAGRANTE E O ACESSO DE DADOS EM DISPOSITIVOS MÓVEIS. NEM UTOPIA, NEM DISTOPIA. APENAS A RACIONALIDADE.



Marcos Zilli

Se as coisas são inatingíveis... ora!
Não é motivo para não querê-las...
Que tristes os caminhos, se não fora
A presença distante das estrelas!
(Mario Quintana)

Esta é a distribuição: uma tonelada tem direitos, um grama tem deveres. Esse é o caminho natural que conduz do nada à grandeza: esquecer que você é um grama e sentir-se a milionésima parte de uma tonelada…
(Ievguêni Zamiátin)

1. ENTRE UTOPIAS E DISTOPIAS PROCESSUAIS

Atribui-se a Thomas More a autoria do termo utopia em romance homônimo publicado em 1516. Em meio à efervescência provocada pelas descobertas, More narra a trajetória de um viajante que se deixa fascinar por uma ilha perfeita onde impera o total bem estar dos indivíduos em ambiente desprovido de propriedade privada e de intolerância religiosa. É possível que a força criativa da alegoria repouse muito antes, mais especificamente em Platão que, na obra *República*, lançou as sementes de uma sociedade fundada nos valores perenes da racionalidade e da justiça. De qualquer modo, é a partir da utopia de More que o conceito ganha força no gênero literário e na filosofia. Projeções idealizadas de sociedades assumem diferentes inspirações e matizes. O distanciamento do real é próprio da utopia, o que não a desqualifica por completo. Afinal, a sua força emana da referência ao real. Nessa perspectiva, indica um ponto ideal de direcionamento do caminhar, ainda que jamais venha a ser atingido. É o "lugar nenhum".

A distopia é o reverso da utopia. É a sua perspectiva obscura, negativa e pessimista. A autoria do termo é atribuída a Stuart Mill por ocasião de discurso proferido no parlamento britânico. Ali, fixou-se o jogo de opostos entre as expressões. A utopia é a tentativa do que é essencialmente bom, enquanto a distopia canaliza o indesejável. No campo literário, a distopia escancarou críticas políticas e sociais, encontrando terreno fértil de criatividade. Ocupam a cena no romance distópico sociedades oprimidas por regimes totalitários que se aproveitam dos avanços tecnológicos para o controle do indivíduo. Não há espaço, portanto, para a intimidade e para a individualidade. Orwell, como se sabe, é ícone da literatura distópica. Mas antes de sua consagrada obra - "1984" -, Zamiátin, escritor russo, já havia brindado o mundo com uma obra de sugestivo título: "Nós". As duas obras tomam as mesmas premissas: sociedades fundadas em uma retórica coletivista em que todos estão submetidos a constante vigilância. Zamiátin descreve casas de vidro que permitem o controle de todos por todos. Em Orwell, a vigilância é feita pelo "Grande Irmão" que tudo vê; tudo observa e tudo controla.

Utopia e distopia carregam exageros. Na primeira, estamos diante do irrealizável, a despeito de ser o desejável. A segunda marca o indesejável, muito embora com riscos de ser concretizável. Aquela deve ser buscada, ainda que inatingível. Esta deve ser evitada, ainda que as tendências apontem em sentido contrário. As expressões, trazidas para o campo da persecução penal, emprestam valoroso material para a reflexão. De fato, os avanços tecnológicos ampliam a capacidade de armazenamento de dados em diferentes níveis. Se de um lado, abrem novos flancos para a execução de ilícitos, de outro ampliam os riscos das devassas dos círculos mais concêntricos da privacidade quando alvo dos tradicionais meios de prova. Os recursos de tecnologia abrem, assim, novos es-

paços de reflexão sobre os seus desdobramentos na persecução penal. A solução não passa, por óbvio, pelos impedimentos absolutos. Fosse assim, a persecução penal seria remetida ao terreno do inviável. Tampouco é possível uma ampliação demasiada das hipóteses de cabimento das medidas. Aqui residiriam os riscos da distopia no processo penal.

2. PROBLEMATIZAÇÃO

Como se sabe, a situação em flagrante confere ao Estado legitimidade de reação imediata a qual se concretiza com a possibilidade de restrição de direitos fundamentais, independentemente de prévia ordem judicial. A prisão e o ingresso domiciliar são os exemplos mais eloquentes. É que o ataque frontal e atual ao mandamento proibitivo justifica a restrição de importantes direitos, o que, diga-se, é próprio de um regime que preconiza o convívio entre as liberdades. Assim, a pronta restrição da liberdade reforça as mensagens de imperatividade da lei e da eficácia do sistema que outorga ao Estado o monopólio do uso legítimo da violência. A relativização da inviolabilidade domiciliar marcada pelo contexto do flagrante delito viabiliza não só a interrupção da prática delituosa, com a preservação de direitos de eventual vítima, como possibilita a obtenção, desde já, de elementos de prova que confiram justa causa às medidas persecutórias. Soa racional, portanto, que da prisão em flagrante decorram a busca e a apreensão de objetos, de instrumentos ou de quaisquer outros bens relacionados com a prática delituosa.

Esse panorama se altera no caso de apreensão de dispositivos móveis em poder de quem está em flagrante? Seria possível o acesso a todos os dados ali registrados, incluindo aqueles que são produto de comunicação? E os demais dados poderiam ser igualmente acessados? A restrição da liberdade decorrente da prisão em flagrante conduz, automaticamente, à restrição de ou-

tros direitos de menor magnitude? Os aparelhos multifuncionais dotados de grande capacidade de armazenamento de dados estariam sujeitos às buscas realizadas em contexto de flagrante delito ou se mostra indispensável a prévia ordem judicial?

Nem de longe as questões são irrelevantes. Afinal, tocam elas a problemática das proibições probatórias. De fato, se se entender impossível o acesso direto aos dados registrados em dispositivos móveis, mesmo que em contexto marcado pela flagrância delituosa, a violação traria a chancela da ilicitude probatória com a consequente imprestabilidade das informações ali colhidas e contaminação das provas derivadas. Como se vê, não são poucas as consequências.

3. PRESENTE, PASSADO E FUTURO DE UM PRECEDENTE (STF, HC 91.867/PA)

A discussão sobre o acesso a dados registrados em aparelhos móveis não é nova. De fato, em 2012, por ocasião do julgamento do HC 91.867/PA[1], o Supremo Tribunal Federal (STF) enfrentou o questionamento sobre a licitude do manuseio de aparelho celular, com o consequente levantamento de dados de ligações registradas, em contexto de prisão em flagrante. O caso é apontado como o precedente[2] sobre a matéria. O cenário nos remete ao ano de 2004 quando da prisão em flagrante de um matador de aluguel. Ao ser preso, os policiais encontraram um aparelho celular que foi, então, por eles manuseado. Naquele momento, foram identificados registros de chamadas efetuadas e recebidas. Uma vez anotados, os números foram

1. Disponível em: goo.gl/u3VQaH Acesso em 07.09.2017.

2. O termo não é aqui empregado na dimensão cunhada pela tradição anglo-saxônica. Ali, os precedentes judiciais guardam uma força vinculatória por parte dos órgãos inferiores de jurisdição. O sistema opera, portanto, nessa dinâmica de certeza, consistência e estabilidade das decisões judiciais justamente por força da forte carga casuística do direito. Neste texto, a expressão "precedente" tem um sentido mais coloquial.

apresentados à autoridade policial que, a partir deles, obteve ordem judicial visando à interceptação das comunicações telefônicas. Durante aqueles procedimentos, os mandantes do homicídio foram identificados. Foram, então, denunciados e presos preventivamente.

A estratégia defensiva buscou a exclusão da prova obtida pelos policiais, a qual foi qualificada de ilícita. Alegou-se que o manuseio do aparelho, sem prévia ordem judicial, teria representado uma afronta à inviolabilidade das comunicações telefônicas. Por via de consequência, o levantamento dos números das linhas telefônicas registradas seria prova inadmissível contaminando todas as demais dela derivadas, vale dizer, a interceptação das comunicações e a revelação de informações sobre o envolvimento dos supostos mandantes no homicídio. A tese, contudo, não foi acolhida pelos sucessivos graus de jurisdição, inclusive no STF.

De fato, ao examinar a questão, o Min. Gilmar Mendes afastou do marco regulatório da interceptação das comunicações telefônicas (Lei Federal n. 9296/96) o acesso dos dados de chamadas efetuadas e recebidas registradas em aparelho móvel. Isso porque o acesso não implicaria invasão de terceiros no espaço reservado da comunicação dos interlocutores tornando desnecessária a prévia ordem judicial. Invocou, ademais, o disposto no art. 6º do CPP o qual concede poderes à autoridade policial para a apreensão de objetos e instrumentos relacionados com a prática delituosa e que sejam encontrados no palco dos acontecimentos. Para o Ministro, a atuação dos agentes policiais teria se jungido aos limites da previsão normativa sem que o manuseio do aparelho tivesse representado uma devassa significativa da privacidade e/ou da intimidade. Nesse ponto, valendo-se da analogia, levantou a hipótese de apreensão de um pedaço de papel contendo anotações referentes a números de linhas telefônicas. Para

ele, a situação imaginada seria comparável ao acesso dos registros das ligações em aparelho celular de modo que não seria razoável afirmar-se para ambos os casos a ilicitude probatória por violação da intimidade[3]. Lembrou, por fim, a previsão constitucional autorizadora da invasão domiciliar para as situações de prisão em flagrante (art. 5º, XI). Para o Ministro, não seria lógico manter-se intacto o respeito à privacidade, impeditivo do acesso aos dados constantes em aparelhos de telefonia móvel, quando o próprio legislador constituinte acena em favor da quebra da inviolabilidade do domicílio em contexto de flagrante delito. Uma conclusão em sentido contrário implicaria proteção mais efetiva aos aparelhos do que à própria moradia, o que não seria minimamente razoável.

3. É o que se extrai do trecho do voto: "*ad argumentandum, abstraindo-se do meio material em que o dado estava registrado, o aparelho celular, indago: e se o número estivesse em um pedaço de papel no bolso da camisa usada pelo réu no dia do crime, seria ilícito o acesso pela autoridade policial? E se o número estivesse anotado nas antigas agendas de papel ou em um caderno que estava junto com o réu no momento da prisão? Ademais, impende lembrar que a CF excepcionou a inviolabilidade domiciliar na hipótese de flagrante delito. A própria liberdade sofre restrição no flagrante delito. Um aparelho celular receberia proteção diversa?*".

Mesmo afirmando a legalidade dos procedimentos que implicaram o manuseio e a obtenção de dados das chamadas efetuadas e recebidas, o Ministro prosseguiu em sua fundamentação, propondo, por absurdo, o reconhecimento da ilicitude daqueles procedimentos. Em seu entender, mesmo assim, as informações que levaram à identificação dos mandantes do homicídio estariam fora do desdobramento ilícito contaminatório. Nesse ponto, considerou perfeitamente aplicável a teoria da descoberta inevitável cujo precedente remonta ao caso *Nix v. Williams,* julgado em 1984 pela Suprema Corte norte-americana. Para o Ministro, caso tivesse se optado pela provocação de ordem judicial, ao invés do manuseio direto do aparelho, inevitavelmente os dados relativos às linhas telefônicas seriam obtidos, fundamentando, assim, o expediente

da interceptação. Ou seja, o curso normal dos acontecimentos conduziria à descoberta daqueles dados que a ação dos policiais apenas antecipou. Nesse raciocínio, para o Ministro a descoberta seria inevitável[4], rompendo-se, dessa forma, a cadeia contaminatória da ilicitude probatória. Assim, ao final e ao cabo, o STF reafirmou a licitude dos procedimentos policiais.

4. Raciocínio que se identifica no seguinte trecho: "Por exemplo, o só fato de serem apreendidos os aparelhos celulares indubitavelmente levaria, como de fato aconteceu, a quebra do sigilo dos dados telefônicos do corréu, com a consequente identificação dos usuários das linhas móveis e fixas que com ele mantiveram contato, mormente na data do cometimento do crime, tramite este, friso, típico e de praxe em casos análogos aos dos autos."

3. STJ, HC 51.531/RO. UM NOVO PRECEDENTE?

É certo que o debate em torno do acesso de dados constantes em dispositivos móveis não se esgotou. Aliás, é provável que se mantenha na centralidade do debate jurídico por muito tempo. A prova eloquente é dada pelo recente julgamento proferido pelo Superior Tribunal de Justiça (STJ) no âmbito do HC 51.531/RO[5]. A situação envolveu a prisão em flagrante de indivíduo que transportava 300 comprimidos de *ecstasy*. Em seu poder, foi encontrado um aparelho celular que foi apreendido e apresentado à autoridade policial. Esta, após o cumprimento das formalidades relacionadas com o flagrante, encaminhou aquele objeto à perícia. Foram, então, levantadas e transcritas diversas mensagens trocadas pelo aplicativo *WhatsApp* cujos conteúdos indicavam tratativas sobre a negociação e o transporte da droga. Assim, foi possível identificar o envolvimento de outras pessoas na ação que, junto com o transportador, foram denunciadas pelo tráfico de drogas em concurso com a associação para o tráfico (art. 33 e 35 da Lei Federal n. 11.343/06).

5. Julgado em 09 de maio de 2016. Disponível em: goo.gl/FNuDv6 Acesso em 09.09.2017.

Mais uma vez veio à tona a alegação de ilicitude probatória. Segundo a defesa, o manuseio do aparelho, sem prévia ordem judicial, implicou devassa de todo o conteúdo ali registrado em clara afronta à privacidade e à intimidade. Pugnou, assim, pela declaração judicial da ilicitude probatória das transcrições das conversas, bem como pelo reconhecimento da contaminação das provas derivadas, afastando-se, por fim, a justa causa para o processamento dos réus. A tese, contudo, não sensibilizou os graus inferiores de jurisdição. A questão foi, então, remetida ao Superior Tribunal de Justiça.

Ao apreciar a matéria, o Ministro Rogério Schietti afastou a aplicabilidade do precedente dado pelo STF quando do julgamento do HC 91.867/PA. Em seu entender, os significativos avanços tecnológicos verificados desde então teriam alterado substancialmente o perfil dos aparelhos de telefonia móvel, o que impediria uma transposição automática dos fundamentos daquela decisão. Nesse ponto, o Ministro destacou o aumento da capacidade de armazenamento de dados das mais diversas origens, fato que potencializou os riscos de devassa da privacidade e da intimidade de seus usuários[6]. Logo, a alteração significativa do cenário justificaria uma nova apreciação da matéria com uma nova ponderação sobre os diferentes interesses em confronto.

Dessa forma, após buscar respaldo em recente julgado proferido pela Suprema Corte dos Estados Unidos (*Riley v. California*), em que se proclamou a indispensabilidade de ordem judicial para o acesso ao conteúdo de dados mantidos em aparelho celular em contexto de prisão em flagrante, o Ministro ressaltou o caráter peculiar daqueles aparelhos, em especial a capacidade de armazenamento múltipla, variável

6. Nesse sentido, destaca-se o seguinte trecho de seu voto: "Os fatos narrados são de 2004, período em que os telefones celulares sabidamente não eram conectados a internet de banda larga, como são já há algum tempo, os chamados smartphones, dotados de aplicativos de comunicação em tempo real, motivo pelo qual o acesso que os policiais teriam àquela época seria necessariamente menos intrusivo do que seria hoje."

e plural de dados. Tais peculiaridades, somadas à proteção constitucional dos diretos à privacidade e à intimidade, com clara projeção na inviolabilidade das comunicações, tornaria indispensável a prévia ordem judicial. Assim, reconhecendo a afronta aos direitos fundamentais, o Ministro declarou a "nulidade"[7] das provas obtidas, determinando o desentranhamento daquelas dos autos do processo.

Em voto concorrente, a Ministra Maria Thereza também proclamou a ilicitude da prova. Nesse ponto, reconheceu o significativo aumento dos riscos de exposição da privacidade e da intimidade propiciada pelos avanços tecnológicos nos aparelhos de telefonia móvel. Assim, também considerou inviável a transposição automática do precedente julgado pelo STF. No entanto, muito embora tenha reconhecido a necessidade de prévia ordem judicial para o melhor controle da invasão à privacidade nos casos de apreensão de aparelhos móveis, a Ministra não conferiu à solução contornos absolutos e definitivos. De fato, não descartou a possibilidade de manuseio daqueles aparelhos diretamente pelos agentes policiais sempre que evidenciada uma situação de urgência que a justificasse, como na hipótese de libertação de vítima em cativeiro. Logo, situações urgentes justificariam uma intervenção rápida e imediata dirigida à proteção de interesses superiores[8]. Uma vez fixa-

7. A rigor a questão é de inadmissibilidade, proclamação que levaria a prova para o terreno da inexistência jurídica. Para além de mera querela terminológica, a distinção entre nulidade e inadmissibilidade no campo das provas ilícitas é mais profunda. Afinal, as nulidades comportam convalidações o que é impossível quando o tema envolve inadmissibilidade da prova. No caso das provas ilícitas, estas ficam permanentemente contaminadas não podendo jamais ser aproveitadas.

8. É o que se verifica do seguinte trecho ora destacado de seu voto: "Não descarto de forma absoluta que, a depender do caso concreto, caso a demora da obtenção de mandado judicial pudesse trazer prejuízos concretos à investigação ou especialmente à vítima do delito, mostre-se possível admitir a validade da prova colida através do acesso imediato aos dados do aparelho celular. Imagine se, por exemplo, um caso de extorsão mediante sequestro em que a policia encontra aparelhos celulares em um cativeiro recém abandonado. O acesso incontinente aos dados ali mantidos pode ser decisivo para a libertação do seqüestrado".

das tais premissas e ponderações, a Ministra voltou-se para o caso objeto do julgamento onde não identificou qualquer situação de risco ou de comprometimento à investigação que não pudesse aguardar uma decisão da autoridade judicial competente. Assim, aderiu ao voto dos demais Ministros para declarar a ilicitude da prova.

4. PARADIGMAS COMPARADOS

4.1 *RILEY VS. CALIFORNIA* (SUPREMA CORTE DOS E.U.A.)[9]

O caso, julgado pela Suprema Corte dos Estados Unidos, envolve, na verdade, duas situações distintas que, no entanto, foram aproximadas em razão do debate comum sobre os limites de acesso a dados constantes de aparelhos de telefonia celular em contexto de prisão em flagrante.

O primeiro envolveu a prisão de Riley ocorrida após uma abordagem de trânsito. Uma vez constatada a suspensão da habilitação, os policiais realizaram os procedimentos de rotina, o que incluía a busca no interior do veículo. Foi quando encontraram armas de fogo, fato que justificou a prisão em flagrante. Nas buscas pessoais, encontraram em poder de Riley um aparelho celular o qual foi prontamente manuseado. Os policiais identificaram, então, referências constantes a uma abreviatura ("CK"), usualmente associada a gangues de rua (*Crip Killers*). Riley foi conduzido ao distrito onde um investigador fez uma pesquisa mais detalhada de seu aparelho celular. Após visualizar alguns vídeos e fotos, o investigador destacou uma imagem na qual Riley aparecia ao lado de um carro. Era o automóvel utilizado durante uma troca de tiros entre gangues, ocorrida semanas antes. Com base nesses elementos, Riley foi acusado por vários crimes, dentre os quais o envolvimento em organização criminosa.

9. Disponível em: goo.gl/zA3WBi Acesso em 02.09.2017.

O segundo caso, submetido ao mesmo julgamento pela Suprema Corte, envolveu a prisão de Wurie. A detenção de Wurie ocorreu após ter sido ele visto no que pareceu ser uma negociação de venda de drogas. No distrito, os policiais apreenderam dois aparelhos celulares. Um deles apresentava em sua tela a indicação de várias chamadas provindas da mesma linha, a qual era referida por "minha casa" (*my house*). O policial, então, acessou os dados do aparelho, identificando o numeral conectado com aquele log. Com o número, identificou o endereço de seu registro. Dirigiu-se até o local e ali confirmou o nome de Wurie na caixa de correio. Ao olhar pela janela do apartamento, avistou uma mulher cuja imagem se assemelhava àquela registrada no aparelho celular. Assim, enquanto manteve o apartamento sob vigilância, obteve um mandado de busca e apreensão. Na execução da ordem judicial, os policiais encontraram mais drogas, além de armas e munições. Wurie foi, então, denunciado pelo tráfico de drogas e pela posse ilegal de arma.

Invocando a violação da IV Emenda[10], que circunscreve a restrição da privacidade à prévia ordem judicial, as defesas tentaram excluir as provas relativas aos dados digitais que estavam registrados nos aparelhos celulares dos réus. No caso de Riley, os argumentos não convenceram os órgãos inferiores de jurisdição. Riley foi condenado a 15 anos de prisão, sentença confirmada pela Corte de Apelações da Califórnia. Wurie foi condenado em primeiro grau. Contudo, o Tribunal Federal (*First Circuit*), por maioria, acolheu a alegação de ilicitude probatória, anulando, assim, o seu julgamento.

No enfrentamento da questão, a Suprema Corte resgatou vários precedentes que fixaram as diretrizes interpretativas da IV Emenda, especialmente os limites permitidos para a

10. Assim redigida: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause,supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

realização de buscas independentemente de ordem judicial. Nesse resgate histórico-jurisprudencial, por assim dizer, foi reafirmada a natureza excepcional das buscas imediatas concretizadas pelos agentes policiais. Assim é que em contexto de prisão, as buscas pessoais estariam autorizadas diante da perspectiva de localização de objetos e instrumentos relacionados com a prática ilícita. Foi o que se decidiu no longínquo ano de 1914 no caso *Weeks vs. United States*[11]. Nos anos subsequentes, a jurisprudência enfrentou a possibilidade de extensão das buscas para além do âmbito corporal para incluir, dessa forma, os espaços de exercício de domínio ou de posse como na hipótese do domicílio do preso. Foi o que se decidiu em 1969, no caso *Chimel vs Califórnia*[12], quando a Suprema Corte reconheceu a extensão do campo de incidência das buscas de modo a se assegurar a obtenção de eventuais provas relacionadas com a prisão.

11. Disponível em: goo.gl/RKgCzv Acesso em 03.09.2017.

12. Disponível em: goo.gl/uFMTTW Acesso em 03.09.2017.

De qualquer modo, no caso dos aparelhos celulares e do acesso aos dados ali armazenados, a Suprema Corte não reconheceu aplicáveis os precedentes. De fato, não considerou sustentável qualquer alegação de risco à integridade dos policiais que justificasse o imediato acesso ao conteúdo registrado e arquivado naqueles aparelhos. Tal conclusão, contudo, não impediria o manuseio do próprio aparelho a fim de se averiguar a possibilidade de acondicionamento de alguma arma ou de qualquer objeto que pudesse ser usado para atacar o policial[13].

13. Conforme ilustra o seguinte trecho que é destacado do julgamento: "Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case".

Já quanto aos riscos de perecimento da prova, a Suprema Corte não se sensibilizou com os argumentos de que os dados poderiam ser suprimidos por aces-

so remoto ou que o acesso pudesse ser obstado por conta de sistemas de segurança criptografados. Nesse ponto, entendeu que as hipóteses não configurariam ameaças reais ou mesmo inafastáveis a ponto de conferir um quadro de razoabilidade a justificar a dispensabilidade da ordem judicial. Com relação a acesso remoto, afirmou que os riscos poderiam ser facilmente afastados com providências simples tais como a desconexão do aparelho da rede de acesso à internet[14]. Com relação aos procedimentos de segurança de criptografia entendeu que estes seriam preexistentes à prisão não se tratando, dessa forma, de um risco fundado no desejo de inviabilizar a investigação, mas sim, de reforçar o próprio espaço de privacidade. De qualquer modo, mesmo para essa situação de criptografia, os juízes da Suprema Corte destacaram a existência de instrumentos e mecanismos que poderiam se não impedir o bloqueio do acesso, ao menos viabilizar o acesso oportunamente[15].

Assim, ao afastar a aplicabilidade automática dos precedentes, a Suprema Corte voltou-se para as especificidades dos modernos aparelhos de telefonia móvel, destacando a multiplicidade de suas funções e a grande capacidade de armazenamento de dados relacionados com os aspectos mais variados da privacidade e da intimidade das pessoas[16]. Entendeu que o acesso àqueles dados fornece uma radiografia precisa sobre a personalida-

14. Conforme ilustra o seguinte trecho da decisão: "In any event, as to remote wiping, law enforcement is not without specific means to address the threat. Remote wiping can be fully prevented by disconnecting a phone from the network. There are at least two simple ways to do this: First, law enforcement officers can turn the phone off or remove its battery".

15. Nesse sentido: "Second, if they are concerned about encryption or other potential problems, they can leave a phone powered on and place it in an enclosure that isolates the phone from radio waves".

16. É o que ilustra a seguinte passagem do julgado: "The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier".

de do usuário, seus gostos, suas preferências e rotinas. Por sua vez, a mobilidade dos aparelhos e, enfim, dos próprios dados não os tornaria mais vulneráveis à proteção emergente da privacidade. Assim, segundo a Suprema Corte, a ordem judicial é providência necessária mesmo que o aparelho seja encontrado em busca incidente à prisão[17]. Não se trata, contudo, de decisão categórica ou absoluta conforme reconhece a própria Suprema Corte. Situações de emergência como a salvaguarda da integridade física de terceiros poderiam justificar as buscas imediatas[18]. Logo, sempre que a demora na obtenção de autorização judicial possa acarretar consequências desastrosas ou mesmo irreparáveis estaria planificada a suficiente razoabilidade suficiente para a restrição da privacidade, independentemente de decisão judicial.

17. O que se evidencia do seguinte trecho que, na verdade, sintetiza a própria decisão: "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple— get a warrant".

18. Nesse sentido: "Such exigencies could include the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury".

4.2 *KEVIN FEARON* (SUPREMA CORTE DO CANADA)[19]

19. Disponível em: goo.gl/uKwKs1 Acesso em 03.09.2017.

Os fatos envolveram o roubo a mão armada de jóias de uma comerciante praticado por duas pessoas. Na fuga, os criminosos fizeram uso de um veículo que foi encontrado pouco tempo depois. Com autorização judicial, os policiais fizeram buscas no automóvel encontrando em seu interior uma arma de fogo. Algumas horas depois do roubo, Kevin Fearon e Junior Chapman foram presos. Nas buscas pessoais, os policiais encontraram, em poder do primeiro, um aparelho celular. Ao acessar os dados nele armazenados, encontraram uma mensagem que fazia referência a algumas jóias. Também encontraram a foto de uma arma de fogo que indicava ser idêntica àquela apreendida no veículo. A Kevin

foi, então, imputada a responsabilidade pelo roubo. Diante disso, invocou a violação à privacidade (art. 8º da Carta Canadense de Direitos e Liberdades)[20].

20. "Everyone has the right to be secure against unreasonable search or seizure".

O argumento, contudo, não foi acolhido pela Suprema Corte em dividida decisão. De fato, a maioria reafirmou a validade das buscas incidentais à prisão, sempre que a obtenção de prévia ordem judicial se mostrar inviável. Trata-se, segundo a posição majoritária, de regra consolidada no pensamento jurídico da *common law*, inspirada pelo princípio da razoabilidade[21]. É que as buscas incidentais viabilizam as investigações preliminares, diretamente conectadas com a prisão, sendo, pois, importantes instrumentos de satisfação do poder punitivo. No entanto, a Suprema Corte não deixou de reconhecer as peculiaridades dos modernos aparelhos de telefonia móvel, destacando a imensa capacidade de armazenamento de dados e os riscos de exposição desnecessária da privacidade. Assim, como forma de balanceamento dos interesses em confronto, propôs a observância de três critérios que melhor orientariam as buscas realizadas no conteúdo armazenado em aparelhos de telefonia móvel em contexto de prisão. Para os juízes, os critérios não representariam obstáculos intransponíveis para as medidas iniciais de satisfação do poder punitivo, tampouco escancarariam o núcleo protetivo da privacidade. Seriam, por assim dizer, formas de composição da eficiência persecutória com o garantismo.

21. Nesse sentido: " 16. Although the common law power to search incident to arrest is deeply rooted in our law, it is an extraordinary power in two respects. The power to search not only permits searches without a warrant but does so in circumstances in which the grounds to obtain a warrant do not exist. The cases teach us that the power to search incident to arrest is a focused power given to the police so that they can pursue their investigations promptly upon making an arrest".

Nesse aspecto, lembraram a necessidade de estreita conexão entre os objetivos da busca e a prisão, exigência que fixa um critério de limitação temporal. Ou seja, apenas as mensagens

mais recentes (rascunhadas, encaminhadas e recebidas), assim como as últimas ligações poderiam ser alvo de exame direto efetuado pelos agentes policiais. Muito embora os juízes tenham reconhecido não se tratar de critério peremptório o qual estaria sujeito a abrandamentos, afirmaram tratar-se de uma orientação a ser atendida com o rigor possível[22]. Por outro lado, afirmaram a validade de interpretações restritivas quando da valoração do critério da necessidade de obtenção de provas. Ou seja, a necessidade de obtenção liga-se às razões que levaram à prisão. Nesse ponto, a Suprema Corte Canadense cita o exemplo da localização de um comparsa[23]. Por fim, os juízes sugerem que as buscas realizadas diretamente pelos policiais sejam alvo de registros os quais haveriam de discriminar o material acessado, bem como o tempo de duração da diligência. A documentação da diligência seria providência que permitiria análises posteriores sobre as razões da ação e os seus limites[24].

5. A PERSPECTIVA DO DIREITO BRASILEIRO

5.1 NEM UTOPIA, NEM DISTOPIA

A busca pessoal vinculada à prisão encontra assento na lei processual (art.

22. É o que se infere do seguinte trecho da decisão: " 76. First, the scope of the search must be tailored to the purpose for which it may lawfully be conducted. In other words, it is not enough that a cell phone search in general terms is truly incidental to the arrest. Both the nature and the extent of the search performed on the cell phone must be truly incidental to the particular arrest for the particular offence. In practice, this will mean that, generally, even when a cell phone search is permitted because it is truly incidental to the arrest, only recently sent r drafted emails, texts, photos and the call log may be examined...".

23. Nesse sentido: "80. A further modification is that the third purpose for which searches incident to arrest are permitted – the discovery of evidence – must be treated restrictively in this context. The discovery of evidence, in the context of a cell phone search incident to arrest, will only be a valid law enforcement objective when the investigation will be stymied or significantly hampered absent the ability to promptly search the cell phone incident to arrest".

24. É o que resta consignado no seguinte trecho: "82 (...) In my view, given that we are dealing here with an extraordinary search power that requires neither a warrant nor reasonable and probable grounds, the obligation to keep a careful record of what is searched should be imposed as a matter of constitutional imperative. The record should generally include the applications searched, the extent of the search, the time of the search, its purpose and its duration".

244 do Código de Processo Penal - CPP), dispositivo este que não afronta o espírito constitucional. Afinal, é intuitivo que outros direitos fundamentais sejam restringidos como forma de viabilizar a privação da liberdade. Com efeito, há que se ter certeza de que o preso não traz consigo, nem levará com ele, instrumentos ou objetos que comprometam a segurança pessoal ou mesmo de terceiros[25]. Trata-se de providência implícita à execução da própria ordem judicial de prisão, razão por que essa busca independe de nova ordem.

É possível aplicar-se o raciocínio para a situação de prisão em flagrante? A resposta é afirmativa. De fato, aqui também a restrição da liberdade implicará restrição de outros direitos e garantias fundamentais incidentais à prisão. Mas nesse caso, as razões não se restringem ao resguardo da segurança do agente que efetiva a detenção. Há, ainda, o interesse de preservação de importantes elementos de convicção ligados à prática delitiva[26]. Ou seja, os fundamentos que autorizam a busca pessoal incidental à prisão em flagrante emergem da motivação política que sustenta esta custódia.

Com efeito, a necessidade de se dotar o aparato estatal de instrumentos de reação imediata para a restauração da ordem pública em face de quem é surpreendido em situação de afronta à norma penal é o que legitima a prisão em flagrante. Insere-se, portanto, no roteiro da violência legítima do Estado a quem cabe o monopólio da atividade persecutória penal. Nesse passo, a exigência de prévia ordem judicial poderia inviabilizar a custódia, fragilizando a mensagem da

25. Conforme pontua Cleunice Pitombo: "...no ato de qualquer prisão, surge imprescindível a revista, para garantir a integridade física do indivíduo, de outros encarcerados e a segurança pessoal de quem o prendeu..." (2005, p.152). Em sentido semelhante: BADARÓ, 2016, p. 499-450 e NUCCI, 2011, p. 562-563.

26. Nesse sentido, pontuava Espínola Filho: "Também, encontrado alguém em situação de ser preso em flagrante, ou dando execução a um mandado regular de prisão, o agente da autoridade não necessita de autorização especial para submeter o preso à imediata busca pessoal, que terá a virtude de pô-lo na posse do corpo de delito, ou de elementos indiciantes de importância". (1945, p. 186).

/ O DEBATE EM TORNO DO ACESSO DE DADOS CONSTANTES EM DISPOSITIVOS MÓVEIS NÃO SE ESGOTOU. /

/ A APREENSÃO TRAZ IMPLÍCITA A AUTORIZAÇÃO PARA O ACESSO IMEDIATO DOS DADOS ALI ARMAZENADOS? /

imperatividade da lei penal, comprometendo, por fim, a autoridade estatal. É natural, portanto, que os agentes de segurança pública estejam autorizados a realizar a busca pessoal em situação de flagrante diante da possibilidade, bastante razoável, de encontro do objeto, dos instrumentos ou mesmo de qualquer outro elemento de prova relacionado com o crime.

Não são outras as razões que levam o legislador constituinte a restringir a inviolabilidade domiciliar em contexto de prisão em flagrante (art. 5º, XI). A restrição se justifica diante da imperiosa necessidade de se fazer cessar a prática ilícita, resguardando, assim, a supremacia da ordem penal. Aqui a ponderação dos interesses conflituosos foi abraçada pelo legislador constituinte que destaca os valores superiores, indicando, a partir de então, a solução. É evidente que a invasão do domicílio implica não só a prisão de quem ali se encontra em situação de flagrante, mas, igualmente, a autorização para a realização da busca pessoal assim como do espaço ocupado pelo agente criminoso, desde que nos limites dados pelo flagrante delito.

Mas, e no caso de encontro de aparelho celular em contexto de flagrante delito? Não parece haver dúvidas quanto à possibilidade de apreensão do aparelho, seja como ato resultante da busca pessoal, seja como ato decorrente da busca domiciliar. O problema, em realidade, é mais profundo. A possibilidade de apreensão traz implícita a autorização para o acesso imediato dos dados ali armazenados?

O contexto sobre o qual se debruçou o STF no que é apontado como o precedente sobre a matéria, definitivamente, não mais se coloca. Isso porque os avanços tecnológicos ampliaram, significativamente, as funções daqueles aparelhos que se tornaram multifuncionais. Para além disso, houve um aumento exponencial da capacidade de armazenamento de dados. De fato, os atuais aparelhos viabilizam a comunicação por diferentes mecanismos, propiciam a troca de arquivos,

em diferentes formatos e configurações, permitem o armazenamento de imagens, vídeos e músicas assim como o acesso, por aplicativos, às informações financeiras e fiscais. São, ainda, instrumentos portáteis que propiciam a navegação pela rede mundial de computadores. Nesse sentido, armazenam o histórico dos sites consultados, revelando, dessa forma, as preferências de seu usuário. Enfim, são usados não só para lazer como também para o desenvolvimento de atividades profissionais com troca e guarda de possíveis informações acobertadas por outros sigilos. É evidente, portanto, a profunda diferença entre os dois contextos. Daí a importância de mais uma indagação: a diferença justifica o encaminhamento de solução diversa daquela tomada pelo STF?

Se por um lado os avanços tecnológicos propiciam novos meios de realização de práticas ilícitas, por outro é inegável a carga lesiva à intimidade que o acesso ilimitado ao conteúdo armazenado nesses aparelhos pode trazer. De fato, é possível traçar não só o perfil do usuário, mas eventualmente de outras pessoas de seu estreito relacionamento. Tais circunstâncias, sem dúvida, devem orientar a melhor solução. Uma restrição absoluta leva à utopia da supremacia da individualidade. Por sua vez, o acesso irrestrito, ainda que incidental à prisão, reduz consideravelmente os espectros de proteção da privacidade.

Nesse ponto, não parece mais válida a analogia feita pelo STF à apreensão de um pedaço de papel com o conhecimento do conteúdo das anotações ali apostas. É que a capacidade de armazenamento de dados dos aparelhos multifuncionais, somada à grande variedade do conteúdo, torna as situações incomparáveis, como de fato o são.

Assim, o acesso ao conteúdo dos *smartphones*, em contexto de flagrante delito, deve se sustentar em situações emergenciais que tornem inviável o aguardo de decisão judicial. As hipóteses dependem da variedade própria da casuística

não sendo possível fixar uma diretriz fechada e restrita. Mas, a localização da vítima, a possibilidade de identificação de comparsas que também se encontrem em situação de flagrante, a possibilidade de se evitar a prática de novo crime e a possibilidade de localização dos objetos da infração são apenas algumas das situações plausíveis. De qualquer modo, e na esteira da orientação dada pela Suprema Corte do Canadá, o acesso deveria ser alvo de registro documental, com a indicação dos dados consultados. A providência tornaria mais fácil o futuro controle judicial sobre a pertinência, legalidade e proporcionalidade da medida tomada diretamente pelos agentes policiais.

A par das situações urgentes, os demais acessos, se necessário forem, deveriam ser alvo de provocação judicial realizada no curso do próprio inquérito que se instaura com a lavratura do auto de prisão em flagrante. Afinal, a lavratura do auto é apenas uma das formas de instauração formal do inquérito. Não encerra a investigação. Deflagra o seu início. Assim, o acesso futuro e a obtenção de novas informações poderão enriquecer o cenário de visibilidade que sustentara a prisão em flagrante, reforçando o quadro da justa causa para o oferecimento da ação penal. A diretriz assim posta melhor posiciona todos os fatores da equação. Não inviabiliza o enfrentamento imediato da situação do flagrante e ao mesmo tempo não escancara as esferas da privacidade a da intimidade.

Há quem, em exegese evolutiva, proponha uma equiparação dos aparelhos multifuncionais ao conceito de domicílio. É uma proposta que busca uma ressignificação deste conceito, livrando-o das amarras que o restringem ao espaço físico em que se projeta a intimidade[27]. A premissa levaria, portanto, à equivalência do grau da inviolabilidade.

Ou seja, a proteção da intimidade dos dados armazenados cederia nas mesmas

27. Nesse sentido: DEZEM, 2017, p. 676-679.

hipóteses em que cede a inviolabilidade do domicílio. Do contrário, haveria uma proteção mais efetiva aos dados armazenados no aparelho do que do próprio domicílio.

A proposta é sedutora. No entanto, ao mover-se mais pelo desejo de articular soluções racionais para as questões, acaba ela por pecar em suas premissas.

De fato, é difícil desconectar da noção de casa a ideia de abrigo e de espaço físico de proteção pessoal, dos familiares e de entes queridos. É um espaço de projeção de várias relações que se desdobram em diferentes graus de abertura (contatos sociais) e de restrição (privacidade e intimidade). Trata-se de uma construção conceitual secular que se manifesta em diferentes sociedades e civilizações. Não parece razoável o redimensionamento de um conceito com fortes raízes históricas, culturais e sociais, por mais que se apresentem revolucionários os avanços tecnológicos. A moradia é um espaço de abrigo que não pode ser transportado por qualquer pessoa. O morador quando ali ingressa, protegido que é pela liberdade reservada, pode dar vazão à sua intimidade e à sua privacidade. E mesmo nesse espaço, poderá estabelecer subníveis de privacidade com restrições ainda maiores de acesso, como no caso de armários ou gavetas trancadas, diários com cadeados, ou mesmo computadores com senhas de acesso. Tem a tranquilidade para assim proceder diante dos limites físicos que estabelecem aquela reserva de liberdade privada. Os domicílios atuais ainda estão distantes daquele desenhado por Zamiátin em seu romance distópico.

Logo, imaginar-se na portabilidade de um aparelho multifuncional, a "portabilidade" do próprio domicílio é metáfora que soa exagerada. Até mesmo porque os aparelhos podem carregar dados que vão além das relações domésticas, como aqueles relativos ao trabalho e, inclusive, de outras pessoas estranhas à relação doméstica. Em realidade, a portabilidade ínsita a esses aparelhos traz a conveniência de se levar con-

sigo uma radiografia de sua própria personalidade em suas múltiplas facetas, relações e interpelações. Assim, a única proximidade possível entre o espaço domiciliar e o conteúdo dos *smartphones* reside nas expectativas que o morador e o usuário possuem, respectivamente, quanto ao resguardo da privacidade e da intimidade manifestadas naqueles espaços.

Aqui reside a importância de um aclaramento. A permissão de invasão do domicílio se dá em contexto de prisão em flagrante justamente porque a casa é um espaço físico delimitado. Nessa hipótese, o ingresso se dá, precipuamente, para interromper a prática delituosa com a prisão de quem se mostra como o seu responsável. E a busca que ali se realiza não é ampla e irrestrita. A autorização de ingresso não implica autorização para a devassa de todo o espaço. Até mesmo porque, como toda e qualquer busca, essa há de ser motivada, orientada e dirigida por uma finalidade que se conecta com a situação do flagrante. Ademais, a cautela há de ser redobrada quando o espaço for ocupado, igualmente, por outros moradores que não tiverem sido marcados pelo selo do flagrante.

Assim, a cautela que direciona a busca domiciliar em contexto de flagrante é a mesma que deve orientar o acesso aos dados armazenados no aparelho. A prisão autoriza a busca pessoal com a apreensão de todos os objetos que estiverem sob a posse direta do preso, dentre os quais o aparelho celular. Mas o acesso ao seu conteúdo deve ser feito à luz da situação de emergência. Este é, portanto, o ponto de convergência que merece a proteção da casa e do aparelho. Ou seja, a aproximação não se dá pela restrição da inviolabilidade, mas sim, pelos limites daquela restrição, vale dizer, pela justa medida de realização dos atos de busca. O fato de a pessoa trazer consigo o aparelho não torna menos protegida a sua privacidade.

Privacidade e intimidade encontram assento constitucional de proteção. A tutela, como se sabe, encontra variados

desdobramentos que não se esgotam nos aspectos expressamente consignados pelo legislador constituinte, como foram a inviolabilidade do domicílio e das comunicações. É fato que o desenvolvimento tecnológico propiciou uma mudança significativa dos canais de comunicação entre as pessoas. O quadro que hoje se mostra é substancialmente diverso daquele com o qual operou o legislador constituinte. Não é possível manter-se intactas exegeses erigidas em outro contexto e que não estabelecem qualquer diálogo com as novas realidades. A interceptação de qualquer ato comunicativo depende, por óbvio, de autorização judicial a qual se materializa, uma vez demonstrada a necessidade e indispensabilidade da medida. O registro das conversas e dos diálogos mantidos encontra-se na linha de desdobramento da privacidade e da intimidade. A inviolabilidade, contudo, não pode ser absoluta. Não é sustentável defender-se a proteção absoluta do conteúdo registrado de uma comunicação e relativizá-la no momento em que ela se concretiza. A projeção temporal da comunicação – contemporânea ou pretérita – não pode ser critério impeditivo da violação da privacidade.

A bem da verdade, a grande questão é a de saber se o acesso àquele conteúdo, incidente à prisão em flagrante e, portanto, independentemente de ordem judicial, seria ou não admissível. Um problema complexo não comporta respostas simplistas e reducionistas. A potencialidade lesiva às esferas da privacidade e da intimidade nos direciona para uma resposta negativa. Mas, de qualquer modo, o impedimento não pode ser peremptório. É que a urgência de certas situações poderá justificar o pronto acesso ao conteúdo das mensagens e dos diálogos registrados. De qualquer modo, há de se ter extrema cautela em tal ponderação. Como meio de obtenção de prova que é o acesso estará sujeito ao controle judicial posterior. Os exageros representam violações aos direitos fundamentais que poderão ser devastadores para o sucesso da persecução penal.

5.2 A VIOLAÇÃO DOS PARÂMETROS DA LEGALIDADE PROTETIVA DA PRIVACIDADE E DA INTIMIDADE: PROVA ILÍCITA E ILICITUDE POR DERIVAÇÃO.

A violação indevida das esferas da privacidade e da intimidade conduz à ilicitude da prova obtida e, por consequência, a sua imprestabilidade processual[28]. A sanção é condizente com um sistema fundado nos valores da dignidade humana. Afinal, a violação escancarada de direitos fundamentais é intolerável, impondo-se a absoluta desconsideração do que dela se obtém. Trata-se de uma "não prova" o que a conduz para o terreno da inexistência jurídica[29]. Não há aproveitamento ou convalidação.

Aliás, os efeitos da ilicitude não se restringem à prova que é obtida diretamente por meios ilícitos. De fato, há uma projeção contaminatória a se considerar. A questão, como se sabe, não é nova, encontrando a sua fonte na jurisprudência norte-americana que consagrou a teoria dos frutos da árvore envenenada – *fruits of the poisonous tree*. A lógica é simples. As provas derivadas de uma prova ilícita original são por ela contaminadas e, portanto, igualmente inadmissíveis. Ocorre que a jurisprudência norte-americana, ao longo das últimas décadas, construiu um complexo sistema de abrandamento dos efeitos da contaminação. Das várias exceções, merecem destaque a "fonte independente" e a "descoberta inevitável"[30].

28. Na dogmática processual brasileira, prevaleceu a teorização construída por Nuvolone (1966) acerca das provas ilícitas e o distanciamento conceitual destas frente às provas ilegítimas. A teoria foi aqui abraçada por Ada Pellegrini Grinover (1982) e, como dito, incorporada pela doutrina processual assim como pela jurisprudência. As provas ilícitas são aquelas obtidas com a violação de direitos fundamentais da personalidade. As ilegítimas, por sua vez, são aquelas produzidas com violação das normas processuais. Aquelas são ilícitas e imprestáveis. Estas podem ser aproveitadas, desde que possível seja a repetição do ato processual que a invalidou. Nesse sentido: ARANHA, 1982; AVOLIO, 2003; FERNANDES, 2010, p. 81-83; MELLO, 2000 e ZILLI, 2013, p. 89-137.

29. GRINOVER; FERNANDES; GOMES FILHO, 2004, p. 170.

30. Ver: LaFAVE; ISRAEL, 1992, p. 473-475 e ZILLI, 2009.

Pela regra da fonte independente, o efeito contaminatório não opera quando a energia proveniente da fonte lícita for superior à energia da prova ilícita original. A hipótese supõe a existência, obviamente, de pelo menos duas fontes que disputam a paternidade, digamos assim, da prova derivada. Se, da análise da situação, concluir-se pela proeminência da fonte probatória lícita, inaplicável será a teoria dos frutos da árvore envenenada[31]. Já pela regra da descoberta inevitável, há, tão somente, a prova ilícita original com os seus efeitos contaminatórios. Se possível fosse concluir que uma prova derivada seria inevitavelmente descoberta, caso o caminho lícito fosse mantido, então não seria possível falar-se em sua exclusão[32].

Diante de tais premissas, fica evidente o equívoco do raciocínio manifestado quando do julgamento do HC 91.867/PA, pelo STF. Naquela oportunidade, o Min. Gilmar Mendes entendeu que os dados armazenados no aparelho seriam inevitavelmente descobertos, caso os agentes tivessem simplesmente apreendido o aparelho, provocando, na sequência, uma decisão judicial autorizadora do acesso. A descoberta inevitável, contudo, rompe o efeito contaminatório entre a ilicitude original e as provas derivadas. Não se trata de regra de convalidação da ilicitude original. Logo, o acesso indevido é que constitui o ponto nevrálgico. Representa o "pecado original" que induz à

31. O caso mais paradigmático é dado pelo caso *O'Bremski*, julgado nos idos de 1967. Uma garota, menor de catorze anos, foi encontrada em um apartamento após uma busca ilegal. Ao prestar declarações, fez referência a diversos abusos cometidos pelo adulto que foi, então, processado. A Suprema Corte afastou a contaminação das declarações prestadas pela menor em decorrência da busca ilegal após reconhecer que a presença da menor no local já era conhecida antes em razão de relatos prestados por informantes antes mesmo do ingresso policial no local.

32. O caso paradigma é o *Nix v. Williams*, julgado pela Suprema Corte em 1984. No caso, um homem, suspeito de matar uma criança, foi interrogado pela Polícia e acabou, em confissão ilegal, admitindo o crime e indicando o local onde o corpo tinha sido deixado. Ocorre que o local por ele indicado já estava sendo vasculhado por dezenas de voluntários. O corpo da vítima foi achado no local indicado pelo criminoso. A Suprema Corte considerou rompido o efeito contaminatório por entender que o corpo seria inevitavelmente descoberto caso a busca pelos voluntários prosseguisse.

imprestabilidade absoluta do material diretamente obtido. A partir deste ponto surge o efeito irradiador da ilicitude. E é sobre este efeito irradiador que se projetam as regras limitadoras da contaminação como é o caso da descoberta inevitável. A aplicabilidade da regra supõe ao menos dois percursos. Um ilícito que se concretiza até o fim. E outro lícito que é interrompido diante da antecipação da ação ilegal. Tome-se, mais uma vez, o precedente do caso *Nix v Williams*. A confissão é a prova ilícita. O encontro do corpo não. Ainda que o local tivesse sido revelado pela confissão, paralelamente existia um movimento lícito – ação dos voluntários – que, se ultimado, levaria à localização do corpo. No acesso indevido aos dados, não há esta opção. É ele a fonte ilícita original.

5.3 A PROVA DOS NOVE. A APLICAÇÃO DAS PREMISSAS AQUI REVELADAS. (STJ, RHC 76324/DF)[33]

O caso envolve a prática de um homicídio em um posto de combustível. No local, os investigadores identificam uma testemunha presencial. Segundo esta, o autor dos disparos, um menor inimputável, teria, antes da execução, conversado longamente com outros indivíduos que estavam do outro lado da avenida. Após a conversa, o menor, munido de uma arma, dirigiu-se até o posto onde baleou a vítima. Com estas informações, confirmadas pelas imagens captadas pelas câmeras de segurança, além das informações relativas aos apelidos dos maiores, prestados pela testemunha presencial que os conhecia pelas alcunhas, os agentes policiais realizam uma rápida pesquisa pelas mídias sociais, identificando, assim, os perfis sociais dos autores mediatos e os seus respectivos endereços. São encontrados e presos em flagrante, momento em que os seus smartphones são apreendidos. Ao vasculharem o conteúdo daqueles aparelhos, os policiais encontram várias

33. Nesse sentido, DEZEM, 2017, pp. 676-679.

mensagens de *WhatsApp*, trocadas entre os maiores, na qual combinavam a atribuição da responsabilidade do homicídio, exclusivamente, ao menor.

O ponto central da discussão pelo STJ envolveu a apreciação da licitude da prova colhida no momento do flagrante, consistente na revelação das mensagens trocadas por aplicativo e armazenadas nos *smartphones* apreendidos. Por unanimidade, entendeu-se não configurada a situação de urgência que tornasse imprescindível o manuseio, desde logo, do conteúdo daqueles aparelhos. Para os Ministros, os elementos até então colhidos conferiam visibilidade suficiente da prática delituosa fundamentando, portanto, a prisão em flagrante que se seguiu. Logo, diante da imperatividade de prévia ordem judicial, o conteúdo das mensagens foi considerado prova ilícita[34].

Ao examinarem o desencadeamento contaminatório, os Ministros entenderam, corretamente, que os elementos de convicção anteriormente obtidos eram independentes já que tinham sido revelados por percurso investigatório não conectado com o desvio ilícito posterior. Assim, entenderam que as demais provas poderiam ser preservadas, em especial os depoimentos prestados pelos investigado-

34. Nesse sentido, destaca-se o seguinte trecho do voto proferido pela Ministra Maria Thereza, relatora do caso: "Com efeito, dos depoimentos que integram o auto de prisão em flagrante não se depreende qualquer fundamento que possa justificar a urgência, em caráter excepcional, do acesso imediato das autoridades policiais aos dados armazenados no aparelho. Para a validade da obtenção dos dados caberia às autoridades policiais realizar a imediata apreensão do aparelho e, subsequentemente, postular ao Poder Judiciário a quebra de sigilo dos dados armazenados no aparelho celular. Não tendo assim procedido, a prova foi obtida de modo inválido".

35. Vale o registro do seguinte trecho do voto da Ministra Relatora: "Posto isso, nos presentes autos, não há qualquer evidencia de que a prova ilícita tenha contaminado nem os depoimentos dos agentes de polícia nem o inquérito policial. De fato, verifica-se dos autos que, em prévia investigação policial, os agentes de polícia compareceram ao local logo após o fato, entrevistaram o dono do estabelecimento comercial onde se deu o ocorrido, bem como seus trabalhadores, levantaram dados sobre a vítima, investigaram a cena do crime, as câmeras do local e localizaram uma testemunha menor de idade que narrou o fato, apontou e descreveu os suspeitos, descrição esta que coincidia com as imagens postadas pelos suspeitos na rede social Facebook, tudo antes de empreender a busca que culminou com a prisão do recorrente e a apreensão do aparelho celular incontinente acessado. E esse prévio trabalho investigativo das autoridades policiais, que culminou com

res e demais testemunhas, o que seria suficiente para conferir justa causa para o inquérito policial e ação penal que se seguiu[35].

a identificação do fato e de seus autores, bem assim como o indiciamento do recorrente, não resta contaminado pelo posterior acesso aos dados do aparelho celular, bastando o desentranhamento dos autos dos documentos extraídos do aparelho celular e a supressão do parágrafo final dos depoimentos policiais, que fizeram referência ao conteúdo das conversas via whatsapp".

6. CONCLUSÕES

< 01 > Os avanços tecnológicos trouxeram transformações significativas nos aparelhos de telefonia celular, dotando-os de multifuncionalidades e de capacidade expansiva para o armazenamento de dados. Assim, a inviolabilidade do conteúdo ali armazenado é projeção do resguardo da privacidade e da intimidade. Não se trata de inviolabilidade absoluta. Restrições são admissíveis, o que é natural em cenário de convívio e de entrechoque de interesses. No entanto, na ponderação dos interesses em conflito não mais é possível focar aqueles aparelhos pelo espelho retrovisor. Isso porque a comodidade trazida pelos *smartphones* aumentou significativamente a potencialidade lesiva às esferas da privacidade e da intimidade, ao mesmo tempo em que abriu novos caminhos para a execução e acobertamento de práticas ilícitas. Logo, as soluções não podem seguir a direção da supremacia da individualidade como também não podem reduzir todas as fronteiras protetivas.

< 02 > A apreensão de *smartphones* em contexto de prisão em flagrante adiciona um novo ingrediente a uma já complexa equação. A visibilidade e a imediatidade da prática ilícita autorizam o Estado, por seus agentes, a adotar medidas que reestabeleçam a ordem pública e o império da lei penal. A restrição da liberdade, na forma de prisão em flagrante, é, portanto,

uma reação legítima do Estado que assumiu o monopólio do exercício da jurisdição penal. A urgência dessa resposta prescinde de prévia ordem judicial, cujo controle é realizado a *posteriori*. A prisão em flagrante traz implícita a restrição de outros direitos fundamentais. A busca pessoal, por exemplo, é indispensável para o resguardo de quem executa a prisão, de terceiros e do próprio preso. A invasão domiciliar, por sua vez, é necessária não só para fazer cessar a prática ilícita, mas também para resguardar a integridade de eventual vítima. Traz implícita, ainda, a autorização para a busca de elementos probatórios que componham o corpo do delito.

< 03 > A apreensão de *smartphones* por ocasião dos procedimentos que cercam a prisão em flagrante é possível. Para tanto, há que se configurar situação justificante daquela restrição, como por exemplo, a presença de suspeitas de que outras provas sobre a prática delituosa possam ali ser encontradas.

< 04 > O acesso ao conteúdo dos *smartphones*, apreendidos incidentalmente em contexto de prisão em flagrante, depende, via de regra, de autorização judicial. Não se trata, por óbvio, de regra peremptória. Situações urgentes pendem o prato da balança para o acesso imediato. A necessidade de localização de vítimas ou de outros comparsas, que também estejam em situação de flagrante, a localização dos objetos da prática criminosa e o impedimento de outras práticas ilícitas, são hipóteses que justificam a ação imediata dos agentes policiais. Não há critérios absolutos. A questão há de ser remetida à jurisprudência que, na singularidade de cada caso, melhor poderá indicar o interesse preponderante.

< 05 > O acesso ao conteúdo, independentemente de ordem judicial, deve ser executado com cautela e nos estritos limites da finalidade que o informa: busca de informações importantes que componham a situação de urgência. É a mesma cautela que deveria orientar a busca domiciliar que se realiza em contexto de flagrante delito. Com efeito, o ingresso autorizado em lei na casa alheia não traz em si uma autorização para uma busca ampla, geral e irrestrita. Ao contrário, a busca tem foco certo e determinado qual seja, aquele indicado pela situação flagrancial.

< 06 > Cuidando-se de medida excepcional, seria conveniente que o acesso imediato fosse alvo de registro por parte dos policiais, discriminando, assim, o conteúdo acessado e as informações obtidas. Trata-se de providência que conferiria maior base e fundamento para um exame judicial posterior sobre a legalidade e proporcionalidade da ação.

< 07 > O abuso evidencia violação ao direito fundamental. A prova obtida é levada para o terreno da ilicitude. É, portanto, imprestável. Não há convalidação possível. Ainda que se obtenha autorização judicial posterior para a obtenção dos mesmos dados que já tinham sido revelados, a prova manter-se-á ilícita. Nesse caso, importante avaliar o desencadeamento do processo contaminatório, vale dizer, a chamada ilicitude por derivação. Também será importante uma análise detida sobre as regras restritivas da contaminação ilícita: fonte independente e descoberta inevitável. Após o enfrentamento de todas estas questões, ter-se-á um quadro mais sólido sobre a permanência ou não de justa causa para o prosseguimento da persecução penal.

7. REFERÊNCIAS

ARANHA, Adalberto José de Camargo. A prova proibida no âmbito penal. *Revista de Jurisprudência do Tribunal de Justiça do Estado de São Paulo*. São Paulo, ano 16,v. 75, mar./abr., 1982, p. 19/24.

AVOLIO, Luis Francisco Torquato. *Provas ilícitas. Interceptações telefônicas, ambientais e gravações clandestinas*. 3. ed., São Paulo: Revista dos Tribunais, 2003.

BADARÓ, Gustavo Henrique. *Processo penal*. 4. ed., São Paulo: Revista dos Tribunais, 2016.

DEZEM, Guilherme Madeira. *Curso de processo penal*. 3. ed., São Paulo: Revista dos Tribunais, 2017.

ESPÍNOLA FILHO, Eduard. *Código de Processo Penal Brasileiro*, 2. ed., v. III, Rio de Janeiro: Freitas Bastos, 1945.

FERNANDES, Antonio Scarance. *Processo penal constitucional*. 6. ed., São Paulo: Revista dos Tribunais, 2010.

GRINOVER, Ada Pellegrini Grinover. *Liberdades públicas e processo penal: as interceptações telefônicas*. 2. ed., São Paulo: Revista dos Tribunas, 1982.

-------; FERNANDES, Antonio Scarance; GOMES FILHO, Antonio Magalhães. *As nulidades no processo penal*. 8. ed., São Paulo: Revista dos Tribunais, 2004.

LaFAVE, Wayne R; ISRAEL, Jerold H. *Criminal procedure*. 2. ed., St. Paul: West, 1992.

MELLO, Rodrigo Pereira de. *Provas ilícitas e sua interpretação constitucional*. Porto Alegre: Sergio Antonio Fabris, 2000.

NUCCI, Guilherme de Souza. *Código de Processo Penal Comentado*. 10 ed., São Paulo: Revista dos Tribunais, 2011.

NUVOLONE, Pietro. Le prove vietate nel processo penale nei paesi di diritto latino. *Rivista di Diritto Processuale*. Padova, v. XXI, p. 442/475, 1966.

PITOMBO, Cleunice. *Da busca e da apreensão no processo penal*. 2. ed., São Paulo: Revista dos Tribunais, 2005.

ZILLI, Marcos. As provas ilícitas no processo penal brasileiro e no

direito penal internacional: duas cabeças, duas sentenças. In. SANTIAGO, Nestor Eduardo Araruna. *Proibições probatórias no processo penal. Análise do direito brasileiro, do direito estrangeiro e do direito internacional*. Brasília: Gazeta Jurídica, 2013, p. 89-137.

-------; We the people..., *Revista Brasileira de Ciências Criminais*. São Paulo, jul./ago., 2009, p. 185-208.

05.

ACESSO A COMUNICAÇÕES ELETRÔNICAS ARMAZENADAS NA PRÁTICA JUDICIÁRIA

Carina Quito

Vinte anos após a entrada em vigor da Lei Federal nº 9.296/96, os limites para o acesso às comunicações eletrônicas, em especial às comunicações armazenadas, são ainda intensamente discutidos, sugerindo a necessidade de regulamentação específica, mais atual e consentânea com essa modalidade de interação humana.

Ao regulamentar a parte final do artigo 5º, XII, da Constituição Federal, a Lei nº 9.296/96 estabeleceu que o sigilo das comunicações (telefônicas ou eletrônicas) em fluxo apenas pode ser afastado por ordem de juiz criminal, presentes indícios da autoria ou participação em crimes apenados com reclusão, desde que não haja meios menos invasivos de se obter a prova. Estabeleceu, ainda, limitação temporal para a execução da medida.

Os requisitos contidos no artigo 2º e a limitação temporal prevista no artigo 5º, ambos da Lei nº 9.296/96, traduzem, em termos legislativos, critérios de proporcionalidade para a restrição à garantia inscrita no artigo 5º, XII. Em vista da necessidade de monitorar comunicações que não deixam registros, e considerando que esse monitoramento implica necessariamente o afastamento de sigilo de conteúdos íntimos que não têm finalidade probatória, o legislador escolheu delimitar de antemão quais situações justificariam a execução de tão invasiva medida cautelar e um prazo[1] razoável de duração.

Diferentemente das comunicações telefônicas, as comunicações eletrônicas deixam registros que podem ou não ser armazenados pelos interlocutores, de modo a torná-las perenes. Com efeito, o afastamento do sigilo sobre as comunicações eletrônicas pode ocorrer sob a forma de interceptação das mensagens

1. Como sabido, a Lei nº 9.296/96 previu prazo de 15 (quinze) dias para a medida, renovável por igual período. A jurisprudência firmou-se no sentido de que esse prazo pode ser renovado tantas vezes quanto necessário, desde que justificadamente. A propósito, ver, por todos, STF, RHC 117467/SP, 1ª Turma, rel. Min. Dias Toffoli, j. 05.11.2013, *DJe* 22.11.2013 e STJ, HC 17910/SP, 6ª Turma, rel. Min. Maria Thereza de Assis Moura, j. 21.11.2013, *DJe* 09.12.2013.

em fluxo, nos exatos moldes da Lei Federal nº 9.296/96, ou sob a forma de apreensão das mensagens já armazenadas pelos usuários em suas contas.

O acesso às comunicações privadas armazenadas encontra-se hoje previsto – embora não regulado – pelo artigo 7º, da Lei nº 12.965/14 ("Marco Civil da Internet"), que prevê a inviolabilidade de sigilo desse conteúdo, salvo por ordem judicial.

A inexistência de menção, no artigo 7º, aos requisitos de quebra já traçados pela Lei nº 9.296/96, aliada à ausência de qualquer outra regulamentação específica para o acesso às comunicações armazenadas, fez despontar, na prática judiciária, grave descompasso entre o grau de proteção conferido às comunicações em fluxo em comparação com as comunicações eletrônicas armazenadas pelos usuários.

A partir de nossa experiência na advocacia criminal, temos observado a prevalência, no Judiciário, de entendimento segundo o qual os requisitos da Lei Federal nº 9.296/96 aplicam-se tão somente às quebras de sigilo de comunicações contemporâneas. Sob essa premissa, e com fundamento no Marco Civil da Internet, prepondera entre os juízes a noção de que o acesso às comunicações eletrônicas armazenadas dependeria de ordem judicial fundamentada, independentemente da finalidade penal da medida ou da natureza do crime objeto de investigação.

Isso significa dizer que são reconhecidos, na prática, critérios mais restritivos para o acesso ao fluxo de e-mails (ou de outras formas de comunicação eletrônica), quando as quebras de sigilo de mensagens armazenadas apresentam-se potencialmente mais invasivas.

Também pela experiência na advocacia, observamos que as ordens judiciais autorizam, em regra, acesso a todo o conteúdo armazenado nas contas, desde a criação, o que equivale, não raro, a anos ou décadas de mensagens enviadas e

recebidas – período muito mais abrangente, portanto, que os 15 (quinze) dias inicialmente previstos na Lei nº 9.296/96.

O julgamento do *habeas corpus* nº 315.220/RS[2] pelo Superior Tribunal de Justiça, em 15 de setembro de 2015, ilustra bem a questão. Debateu-se, por meio da ação impugnativa, a ilegalidade da quebra de sigilo de correio eletrônico que abrangeu comunicações armazenadas no período compreendido entre os anos de 2004 a 2014[3].

Como demonstra o caso julgado, existe em relação ao conteúdo armazenado nítida tendência à autorização de quebras desmedidas, tanto em função da natureza do fato a ser provado (fato que não tem relevância penal ou que constitui crime de menor potencial ofensivo), quanto em função da abrangência temporal do acesso às comunicações.

Sobre o último ponto, deve-se ter em mente que, para se executar a medida, afasta-se primeiro o sigilo de todo o conteúdo armazenado por anos para, depois, buscar-se dentre as mensagens apreendidas aquelas que têm alguma relevância probatória.

A noção de que a proteção constitucional conferida pelo artigo 5º, XII tem por objeto apenas o processo comunicante e de que as comunicações eletrônicas armazenadas estariam abrangidas pela garantia geral à intimidade (artigo 5º, X) está no cerne do problema aqui tratado, pois afasta as quebras de conteúdo armazenado do âmbito de incidência da Lei Federal nº 9.296/96, deixando a critério dos juízes, em cada caso concreto, decidir o que seria ou não uma quebra de sigilo dotada de proporcionalidade.

2. STJ, 6ª Turma, *Habeas Corpus* nº 315.220, rel. Min. Maria Thereza Rocha de Assis Moura, j. 15.09.2015, *DJe* 09.10.2015.

3. Na análise do caso, o Superior Tribunal de Justiça assentou que "*para se afastar a arbitrariedade da constrição, considerando-se que a Lei nº 9.296/96 não dispôs prazo máximo limite para a providência, apresenta-se clarividente a subordinação do decisum judicial à necessidade de proporção da medida*". Concluiu-se, assim, que o extenso período da quebra mostrava-se desproporcional à finalidade probatória da medida ordenada pela autoridade coatora.

/ DIFERENTEMENTE DAS COMUNICAÇÕES TELEFÔNICAS, AS ELETRÔNICAS DEIXAM REGISTROS QUE PODEM TORNÁ-LAS PERENES. /

/ NÃO HÁ COMO JUSTIFICAR MAIOR GRAU DE PROTEÇÃO A COMUNICAÇÕES EM FLUXO DO QUE ÀQUELAS ARMAZENADAS. /

A nosso ver, o conteúdo das interações humanas é o objeto da proteção constitucional do artigo 5º, XII. Não há como se distinguir, sob essa ótica, comunicações em fluxo daquelas armazenadas[4], não se justificando menor grau de proteção às comunicações que o usuário opta por manter registradas, porém ocultas de terceiros.

Sob esse mesmo prisma, entendemos que, no atual cenário normativo, as quebras de sigilo de comunicações eletrônicas armazenadas devem ser pautadas nos mesmos critérios estabelecidos pela Lei nº 9.296/96 para as interceptações das comunicações em fluxo, o que restringe a apreensão de e-mails armazenados à persecução das infrações penais apenadas com reclusão, em não havendo outros meios menos invasivos de obtenção de prova, pelo período delimitado no artigo 5º, ainda que ampliável sucessivamente por decisões judiciais justificadas.

A prevalecer o entendimento de que as mensagens armazenadas receberiam a proteção da cláusula geral de intimidade (artigo 5º, X da Constituição), em virtude do potencial de devassa na vida privada, despontaria, a nosso ver, necessidade urgente de se regulamentar o artigo 7º do Marco Civil da Internet para se equiparar a proteção conferida às comunicações armazenadas àquela que é dispensada ao fluxo de e-mails.

Regulamentação nova e específica deveria, no mínimo, condicionar o acesso ao conteúdo armazenado à investigação ou instrução processual de crimes mais graves ou taxativamente expressos em lei, limitando os acessos ao período estritamente necessário para a obtenção da prova.

4. Nesse ponto, concordamos integralmente com Ricardo Sidi (*A interceptação das comunicações telemáticas no processo penal*. Belo Horizonte, D´Plácido, 2016, p. 300). Segundo o autor, "não há coerência ou razoabilidade em retirar os e-mails armazenados do âmbito de proteção do direito ao sigilo de comunicações (art. 5º, XII, CF). *Afinal, por mais que sua arrecadação já não caracterize uma interceptação propriamente dita, por falta do requisito contemporaneidade, e por mais que se trate de mensagem já recebida pelo destinatário, é inegável que a preservação de seu conteúdo humano e demais detalhes ligados a ele não pode ser dissociado da expressão constitucional 'sigilo das comunicações', dotada de tão claro sentido linguístico*".

06.

O DEBATE ESTADUNIDENSE SOBRE VIGILÂNCIA E CRIPTOGRAFIA

Riana Pfefferkorn

Tradução de Ana Luiza Araujo. Revisão técnica de Jacqueline de Souza Abreu.

Estou muito honrada por ter sido convidada para falar com vocês sobre o tópico de hoje, que é o debate nos Estados Unidos sobre as tensões entre a criptografia e o cumprimento da lei (*law enforcement*). Este debate é fundamentalmente um debate sobre poder – quem pode ter, quem decide quem tem, quem quer ou não quer ter e por quê, e para que é usado.

Os seres humanos são animais que fabricam ferramentas. Nós inventamos novas ferramentas – novas tecnologias – como forma de empoderamento. Novas tecnologias têm o propósito de nos ajudar a fazer as coisas que fazemos – de uma maneira melhor, mais rápida, mais forte, mais eficiente, em maior número. E elas nos permitem fazer novas coisas que nós não podíamos fazer antes de maneira alguma. Isso acontece com o telefone, com a máquina de lavar e com uma metralhadora.

Cada uma dessas tecnologias muda a quantidade de poder que seu usuário detém. Então quem tem essas ferramentas se torna muito importante – especialmente se você é alguém com mais poder do que os outros, e quer se manter dessa maneira.

Muitas novas tecnologias não são disponíveis para o público leigo, principalmente assim que são inventadas. Talvez elas sejam mantidas em segredo, assim o seu inventor tem uma vantagem militar – por exemplo, como fazer armas nucleares – ou uma vantagem econômica – como fazer Coca-Cola. E ainda que não seja um segredo, uma nova tecnologia ainda pode ser muito cara em um primeiro momento – o que a mantém fora de alcance para pessoas comuns.

Mas segredos são revelados e os preços caem. Quando uma tecnologia se torna acessível a todos, não apenas aos militares, ou à elite, ou a alguns poucos negócios a mando do Rei, é então que as pessoas que detêm o poder começam a ficar nervosas. Isso acontece porque a tecnologia diminui a lacuna de poder entre eles e você. É por isso, por exemplo,

que a Inglaterra costumava requerer licenças para prensas de impressão. Ou porque a Arábia Saudita ainda não permite que mulheres dirijam.

E é por isso que autoridades de investigação, tanto no seu país quanto no meu, estão tão nervosas com a criptografia. O debate sobre criptografia é o mais novo capítulo na história secular do desconforto de autoridades com o acesso popular a tecnologias que empoderam as pessoas para exercer seus direitos humanos, como privacidade e liberdade de expressão.

ACESSO PARA MIM, MAS NÃO PARA TI

A polícia está acostumada a ter acesso. E eles estão acostumados ao acesso ser a coisa *deles*, não a *sua* coisa. Eles estão acostumados a poder ficar de olho nas suas comunicações e nos seus dados. E eles estão acostumados com que a maioria das pessoas não consiga efetivamente deixá-los de fora.

Mas devemos lembrar que o seu acesso "*habitual*" não é algo ao qual o Estado tem direito por alguma lei natural ou ditado Divino. As Constituições e leis de nossos dois países determinam o que as autoridades de investigação podem ou não podem fazer. Se autoridades de investigação querem acesso às informações de alguém, a Constituição e as leis dizem quais informações elas têm permissão para ver e qual a maneira correta de obtê-las. Mas essas leis não são sobre a *habilidade* da polícia de acessar a informação. Elas apenas dizem à polícia quais são os *passos procedimentais* que eles devem seguir para consegui-la. Que é *possível* consegui-la é considerado dado.

É isso que a criptografia muda. As autoridades de investigação estão acostumadas a *conseguir acessar* informações com o processo judicial correto. Tornar a criptografia comercialmente disponível para o público em geral debilita a *habilidade inerente* da polícia em acessar informações mesmo com a autorização legal apropriada.

AS GUERRAS DE CRIPTOGRAFIA NOS EUA NOS ANOS 90

A primeira grande ameaça à essa capacidade nos Estados Unidos veio no início dos anos 1990, quando o setor privado começou a seriamente desenvolver softwares para o uso comercial que incluíam a criptografia como um recurso. As autoridades de investigação e as comunidades de inteligência não ficaram felizes. O governo norte-americano tentou controlar a criptografia disponível comercialmente, tanto domesticamente quanto no exterior. Nós chamamos esse período de "Guerras de Criptografia".

Do lado internacional, os EUA regularam a criptografia como uma munição e controlaram estritamente a sua exportação para outros países. Os EUA estavam acostumados a serem a superpotência do mundo, um status mantido em parte pelo seu exército e pelos seus serviços de inteligência. Se outros países tivessem uma criptografia tão forte quanto a norte-americana, então nós não poderíamos espionar vocês tão bem quanto antes. Algumas empresas americanas responderam oferecendo duas versões de seu software: uma para usuários norte-americanos como eu, e outra com uma criptografia mais fraca para usuários internacionais como vocês.

Mas isso não é dizer que os EUA estavam totalmente confortáveis com os cidadãos americanos tendo acesso a uma criptografia mais forte. Domesticamente, a Agência de Segurança Nacional (NSA) tentou fazer o setor privado adotar um dispositivo chamado "Clipper Chip", que criptografaria chamadas telefônicas – mas possuía um *backdoor* implantado para acesso do governo.

Porém, no fim dos anos 1990, tanto os esforços estrangeiros, quanto os domésticos haviam falhado. O "Clipper Chip" nunca foi adotado por causa de reações de ativistas de privacidade e a descoberta, por respeitados especialistas em criptografia, de vulnerabilidades críticas em seu protocolo de criptografia. Os

controles sobre a exportação foram gradualmente atenuados por conta de pressões econômicas paras manter os EUA competitivos no mercado global. Também houve disputas legais nos tribunais, contestando que as restrições de exportação violavam a liberdade de expressão. E, no fim das contas, você não pode colocar o gênio de volta na lâmpada. A criptografia havia se tornado disponível para o público em geral, e ela estava aqui para ficar. As "Guerras de Criptografia" foram vencidas.

CALEA: UM EMPATE NAS BATALHAS DE CRIPTOGRAFIA DOS ANOS 90

Foi durante esse período do início dos anos 1990 que nós começamos a ouvir o primeiro alarme soado pelas autoridades de investigação norte-americanas sobre a percepção da ameaça de criminosos protegerem suas atividades de detecção utilizando meios tecnológicos, incluindo a criptografia. O nome dado pelos oficiais americanos a essa ameaça foi "autoridades ficando no escuro" (do inglês, "Going Dark").

Nossa agência federal de investigações, o Federal Bureau of Investigation (FBI), levou essa preocupação até o Congresso, que, em 1994, aprovou um estatuto federal chamado Ato de Assistência de Comunicações para autoridades de investigação, ou CALEA (sigla do inglês) para encurtar.

O CALEA exige que operadoras de telecomunicações façam suas redes e equipamentos tecnicamente capazes de serem monitorados por autoridades de investigação. Isso garante que quando as autoridades de investigação conseguem uma ordem judicial autorizando-as a escutar as conversas telefônicas de um alvo, ou gravar os números para quem ele liga ou é chamado, os agentes poderão ir até a operadora e implementar aquela ordem.

Mas existiam três limitações importantes ao CALEA quando ele foi aprovado:

< 01 > ele não permite que as autoridades de investigação determinem ou proíbam designs específicos para os equipamentos, estabelecimentos, serviços ou recursos das operadoras;

< 02 > como originalmente escrito, ele isentava "serviços de informação", o que significa a Internet, e

< 03 > ele diz que as operadoras "não são responsáveis pela decifragem das comunicações que seus clientes criptografarem, a não ser que a operadora tenha fornecido a criptografia E possua as informações necessárias para decifrar a comunicação". Ou seja, as operadoras estão livres para oferecer uma criptografia que elas não têm a habilidade de remover. [47 U.S.C. § 1002(b).][1]

Essas limitações foram o resultado de uma intensa luta entre autoridades de investigação, especialistas em segurança, e grupos de defesa das liberdades civis pela linguagem e a abrangência do CALEA. O CALEA reflete um equilíbrio que os membros do Congresso, que teriam que dar explicações ao público, alcançaram entre interesses concorrentes incluindo ordem pública, segurança e privacidade. O processo envolveu montanhas de evidências e depoimentos de especialistas. O resultado foi algo que, para as autoridades de investigação, foi uma preservação de seu poder, mantendo o *status quo*. Mas muitos nas comunidades de liberdades civis acharam que esse comprometimento cedeu

1. [Nota da editora] (b) Limitations. (1) Design of features and systems configurations. This subchapter does not authorize any law enforcement agency or officer— (A) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services; or (B) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services. (2) Information services; private networks and interconnection services and facilities. The requirements of subsection (a) do not apply to—(A) information services; or (B) equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers. (3) Encryption. A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.

muito espaço, apesar dos cortes. Além disso, uma década depois, o FBI expandiu o CALEA para abranger provedores de banda-larga de Internet e alguns provedores de VoIP, o que decepcionou ainda mais a comunidade dos direitos civis.

Esse não foi o fim dos esforços do FBI para expandir o CALEA. Em 2010, o FBI pressionou o Congresso a forçar *todos* os sistemas de comunicação (como Gmail ou Facebook), incluindo todos os softwares de criptografia, a incluir *backdoors* para o acesso de autoridades de investigação. Eles citaram o problema do "Going Dark" em uma época de onipresença de serviços baseados na Internet. A proposta de lei morreu depois de um levante popular. Em 2013, o FBI novamente incitou o Congresso, novamente em vão, para estender o CALEA a todos os serviços de comunicação, para que então empresas com serviços de mensagens tivesses que criar *backdoors* em seus produtos e decifrar todas as mensagens encriptadas.

Estes são episódios que conectam as Guerras de Criptografia dos anos 1990 à nova guerra de criptografia. Se aprovadas, as propostas do FBI teriam desfeito duas das três isenções que foram trabalhosamente tiradas do CALEA em 1994: a retirada da Internet e a retirada da criptografia. O FBI já havia tirado um pedaço desta última através da extensão para banda-larga e VoIP, e em 2010 e 2013, eles tentaram terminar o serviço. Mas em seus esforços de relações-públicas, o FBI pintou essas campanhas para estender o CALEA meramente como uma tentativa de preservar o *status quo* do acesso às comunicações dos americanos, não como uma expansão dos poderes das autoridades de investigação.

SETEMBRO DE 2014: APPLE APRESENTA O IOS 8

Essa era a mentalidade que a comunidade de autoridades de investigação ainda tinha até setembro de 2014, quando a

nova guerra criptográfica realmente começou. Isso foi quando a Apple anunciou o iOS 8 para o iPhone. Começando com o iOS 8, a Apple iria fornecer uma criptografia padrão para iPhones que nem a Apple poderia contornar para autoridades de investigação.

Nas versões anteriores 4-7 do iOS, a Apple poderia contornar a senha do usuário e extrair certas categorias de dados nos termos de uma ordem judicial. No iOS 8, os arquivos no aparelho são protegidos por uma chave de criptografia que mistura a senha do usuário, que a Apple desconhece, com a identidade única do aparelho, que a Apple também desconhece. Resumindo: mesmo que a polícia tenha um mandado para revistar um iPhone, a Apple não poderia mais desbloqueá-lo.

As autoridades de investigação norte-americanas ficaram *furiosas*. James Comey, que há até algumas semanas atrás era o diretor do FBI, foi à imprensa e ao Congresso. Seus avisos ecoavam o que o FBI havia dito em suas tentativas de expandir o CALEA. Isto é, que terroristas e pedófilos "iriam para a escuridão", dessa vez com a ajuda da Apple.

A retórica era totalmente das Guerras de Criptografia dos anos 1990 de novo. Mas dessa vez, não era apenas o acesso às comunicações que preocupava o FBI. Com o iOS 8, o problema era a criptografia para dados em repouso nos nossos agora-onipresentes smartphones.

Assim como nos anos 1990, a atitude das autoridades de investigação em relação ao iOS 8 era de que elas estavam sendo *privadas* de algo para o qual elas tinham um *direito* sob o *status quo* que garantia a elas o acesso a esses dispositivos. Mas isso não era assim. Esta fonte de prova não existia por causa de um edito dado por Deus ou pela ordem natural das coisas. A Apple voluntariamente começou a fazer iPhones em 2007, e eles rapidamente se tornaram um baú do tesouro de informações coletadas em um lugar que cabe no bolso.

Claro que as autoridades de investigação amaram isso. Mas os investigadores apenas tinham acesso aos dados em iPhones porque a Apple decidiu produzi-los daquele jeito. Eles eram livres para tomar essa decisão. E agora, com o iOS 8, a Apple decidiu deixar de fazer isso. Eles eram livres para tomar essa decisão também. A Apple continuaria a cumprir mandados de busca e ordens judiciais até onde eles puderem. Mas agora eles não poderiam contornar a sua própria avançada criptografia. A Apple havia mostrado esses baús para os agentes, e agora estava empurrando-os para longe.

Se os iPhones não fossem tão populares, isso não teria importado tanto para o FBI e seus colegas. Como eu disse, o que assustava os agentes sobre a criptografia nos 1990 era que ela se tornaria prontamente disponível em softwares e hardwares comercialmente disponíveis. As autoridades de investigação estão acostumadas a ter acesso às suas informações. Mas elas não estão acostumadas a você tendo um fácil acesso a maneiras de proteger as suas informações.

Mas o mundo não acabou depois dos anos 1990, apesar do relaxamento dos controles de exportação e a isenção do CALEA para criptografia. Sim, a criptografia disponível comercialmente se tornou amplamente utilizada para assegurar o tráfego na Internet, *e-commerce*, transações bancárias, e coisas do tipo. Mas a criptografia não era *assim* tão comumente usada por consumidores para laptops ou dispositivos móveis ou enviar mensagens ou navegar na rede. Você tinha que achar uma ferramenta que funcionasse nos seus equipamentos e então você tinha que aprender como instalá-la, configurá-la, e usá-la corretamente. Produtos de criptografia são há muito tempo *bastante* não-amigáveis ao usuário no seu design. Eles fizeram com que criptografar coisas fosse um pé no saco, então a maioria das pessoas não se importou.

Mas pelo o que a Apple é conhecida? Um design limpo e facilidade de uso. Agora, em 2014, a Apple havia usado essa expertise levando criptografia de aparelhos (*device encryption*) para o altamente popular iPhone. De repente, *milhões* de pessoas teriam fácil acesso a uma criptografia forte para a vasta quantidade de dados mantidos em seus smartphones, usando apenas uma senha de poucos caracteres. Eles não tinham que assertivamente procurar, baixar, e instalar um software especial. Eles não tinham que fuçar menus de configuração. Ela Apenas Funcionava.

Isto é o que assusta as autoridades de investigação norte-americanas, e, eu estou disposta a apostar, os agentes brasileiros também. Quando era diretor do FBI, James Comey reconheceu que criminosos e terroristas determinados e sofisticados sempre irão encontrar um caminho para ter acesso à criptografia, não importa o que a lei americana diga ou o que a Apple faça. Mas esses indivíduos serão comparativamente raros. A *maioria* dos criminosos vai continuar não sofisticada, e eles são os envolvidos em crimes do *dia-a-dia*. Com uma criptografia forte disponível por padrão em um smartphone, a polícia pode não conseguir acessar um telefone quando *pessoas medianas* cometem *crimes medianos* – o ganha-pão diário de policiais e promotores. Criptografia *padrão* em dispositivos para *consumidores* em uso *generalizado* é um divisor de águas.

LEGISLANDO CONTRA O "GOING DARK"? NÃO TÃO RÁPIDO ASSIM

E isso é perfeitamente legal. Sob a lei estaduindese, a Apple é livre para desenvolver o iOS como ela desejar. Não há uma lei dizendo que a Apple não pode desenvolver seus telefones com uma criptografia forte, ou requerendo que a Apple apenas coloque uma criptografia fraca e com *backdoors*, ou que de outra

maneira garanta o acesso para as autoridades de investigação. A árvore plantada nos anos 1990 durante as primeiras rodadas das Guerras de Criptografia finalmente deu seus frutos. A Apple tem a liberdade de fazer um smartphone que ela não possa abrir para a polícia, mesmo com um mandado.

O anúncio de 2014 do iOS 8 virou a mesa no antigo *status quo* do "acesso para mim, mas não para ti". A tampa do baú do tesouro estava se fechando. O que fazer?

Bem, fazer o iOS 8 não era ilegal, mas talvez isso pudesse mudar. O Sr. Comey e seus colegas propuseram passar uma lei para *forçar* o *status quo* de volta para como a Apple o tinha *voluntariamente* estabelecido pré-iOS 8. Comey e outros oficiais exigiam que a legislação requeresse que fabricantes de telefones construíssem *backdoors* na criptografia dos dispositivos, ou então que encarassem multas criminais. A ideia era de que as autoridades pudessem usar esses *backdoors* para acessar dados encriptados, mas que os *backdoors* não poderiam de maneira alguma serem usados por caras maus.

Os agentes de segurança defendendo essa ideia não ofereceram nenhum detalhe técnico específico de como isso funcionaria. Eles deixaram essa parte para os nerds do Vale do Silício. Mas a ideia soava como um Clipper Chip 2.0, e ela foi tão denunciada por especialistas em criptografia quanto a primeira. As autoridades de investigação tentaram retratar as empresas do Silicon Valley como sendo teimosas e relutantes em criar uma solução que poderia ser totalmente inventada se eles apenas trabalhassem arduamente. Especialistas em criptografia responderam que isso não era sobre teimosia. O que os agentes queriam era simplesmente impossível.

Se você coloca um *backdoor* no seu software de criptografia, ele não pode ser apenas limitado aos caras bonzinhos. Ele pode e será usado pelos caras maus também. Criptografia é apenas matemática. Ela simplesmente não funciona de uma

maneira para a polícia e pessoas inocentes, e de outra para criminosos. A matemática funciona do mesmo jeito para todo mundo. Para as autoridades obcecadas com as dinâmicas do poder, aparentemente isso é muito difícil de entender.

Até agora a abordagem legislativa para lidar com o problema do "Going Dark" nos Estados Unidos não foi a lugar algum. O Presidente Obama foi surpreendentemente indeciso sobre o "Going Dark", a despeito de uma petição popular enviada à Casa Branca pedindo que tomasse ações para defender a criptografia. Em 2015 e 2016, projetos de lei do tipo "CALEA versão II", demandando que a criptografia de dispositivos móveis fosse acessível para autoridades de investigação, foram introduzidos em três estados dos Estados Unidos: Califórnia, Nova York e Louisiana. Nenhum desses projetos foi a lugar algum. Dois senadores no Congresso Federal, incluindo um dos senadores pela Califórnia – casa das grandes empresas de tecnologia – escreveram um projeto de lei em 2016 que determinaria que as empresas fossem capazes de cumprir ordens judiciais para decifrar informações. Um anteprojeto da lei circulou. O anteprojeto era tão mal escrito, e a ideia por trás era tão ignorante e imprudente, que o projeto nunca nem chegou a ser formalmente apresentado porque os protestos de especialistas em criptografia e defensores das liberdades civis foram muito ágeis e intensos.

Então, até a eleição presidencial em novembro de 2016, Comey, o diretor do FBI, parecia ter desistido da ideia de uma "solução legislativa" para o "Going Dark". Ao invés disso, ele disse, as autoridades de investigação teriam conversas com as empresas de tecnologia para tentar persuadi-las a voluntariamente alterar seus produtos. Em vez de um processo legislativo aberto, conduzido em público por políticos que têm responsabilidades com seus constituintes, Comey planejou botar pressão em empresas como a Apple atrás de portas fechadas.

Mas ele mudou sua história depois da eleição. Ele não havia tido sucesso com Obama, mas Comey disse que ele havia planejado levar o problema do "Going Dark" novamente para o Congresso e o novo presidente. Talvez 2017 fosse diferente.

Bom, 2017 está muito diferente. O novo presidente demitiu o Sr. Comey no início de maio. Até agora – a não ser que algo tenha sido reportado desde que eu comecei a falar, o que é totalmente possível – nós não sabemos quem vai substituir Comey como diretor do FBI. Ninguém parece querer o trabalho, por alguma razão. Então não está claro qual será a posição de seu sucessor quanto a "Going Dark".

Dito isso, eu duvido que o novo diretor do FBI seja *mais* amigável à criptografia. O novo diretor será indicado por um presidente que não tem interesse em problemas tecnológicos ou em políticas públicas complexas, e que, durante a campanha, pediu o boicote da Apple pela sua recusa a ajudar agentes de segurança no cumprimento da lei. Por outro lado, nosso Congresso andou muito ocupado com outras coisas (algumas delas também envolvem o Sr. Comey, que supostamente deve depor logo no Congresso). E o povo estadunidense está politicamente engajado de uma maneira que não vemos há anos – e nós amamos nossos iPhones. Então a legislação para o "Going Dark" que Comey queria provavelmente não vai acontecer tão cedo, se isso.

"GOING DARK" NOS TRIBUNAIS: O *ALL WRITS ACT*

Então esse é o cenário legislativo. Neste momento, a criptografia é legal nos Estados Unidos. Ponto final. Mas o Legislativo é apenas um dos braços do governo. As autoridades de investigação têm perseguido a pauta do "Going Dark" também nos tribunais.

Diferentemente do Brasil, os Estados Unidos têm um sistema de *common law*, não um sistema de *civil law*. Isso significa que os tribunais dependem fortemente de decisões judiciais já publicadas de casos anteriores, similares. Então, em um sistema de *common law*, a decisão de uma corte federal dizendo que a lei autoriza o FBI a conduzir um certo tipo de vigilância é muito valiosa para o FBI, porque eles podem apontar para essa decisão na próxima vez em que eles forem a outra corte federal para pedir outra autorização de vigilância em outra investigação.

E o FBI tem ido com bastante frequência aos tribunais por iPhones criptografados. Eu vou falar sobre o caso "Apple vs. FBI" daqui a pouco, mas essa não foi a primeira vez em que o FBI foi aos tribunais para fazer com que a Apple os ajudasse a acessar um iPhone criptografado. Pelo menos desde 2008 até o fim de 2015, agentes policias conseguiram dezenas de ordens de juízes federais dizendo à Apple que contornasse a senha em iPhones pré-iOS 8 para os quais eles possuíam mandados [*warrants*]. Eu vou relembrá-los de que isso é algo que a Apple ainda podia fazer pré-iOS 8. Esses procedimentos judiciais aconteceram sob sigilo. Assim como reuniões privadas com empresas, ir aos tribunais sob sigilo levou o governo a operar fora da luz do debate público.

Em suas petições para os tribunais, os advogados do governo não citaram nenhuma lei especificamente autorizando a ordem de desbloqueio para a Apple que eles buscavam. Isso aconteceu porque não existe uma, e algumas vezes eles admitiam isso. Ao invés disso, eles argumentavam que a ordem requisitada era autorizada pelo *All Writs Act* (AWA), uma lei de 1789. O AWA age como uma autoridade residual preenchedora de lacunas totalmente abrangente, permitindo com que um tribunal emita mandados [*writs*] que de outra maneira não seriam cobertos pela lei. Ele diz que as cortes federais podem

"emitir todos os mandados necessários ou apropriados em auxílio de suas respectivas jurisdições e em concordância com os usos e princípios da lei".[2]

2. "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C § 1651(a)

Nos anos 1970, as autoridades usavam o AWA para conseguir autorização para instalar dispositivos chamados de "*pen registers*" em sistemas de companhias telefônicas. *Pen registers* gravam todos os números discados de uma linha telefônica sob investigação. A Suprema Corte defendeu esse uso do AWA em um caso de 1977 chamado *United States vs. New York Telephone Co.* (434 U.S. 159). Desde de 1986, os Estados Unidos têm uma lei federal específica para *pen registers*.[3] Mas o caso da *Companhia Telefônica de NY* ainda vale. E no nosso sistema de *common law*, a interpretação da Suprema Corte sobre o AWA vincula todas as cortes abaixo dela.

3. [Nota da editora] U.S.C. §§ 3121-3121. Disponível em: goo.gl/sPJM8N

Por isso, décadas depois, autoridades federais ainda estavam usando o caso da *Companhia Telefônica de NY* para tentar persuadir juízes federais pelo país de que a AWA autorizava uma ordem exigindo que a Apple providenciasse assistência técnica no desbloqueio de iPhones. Ainda que a Apple fosse uma terceira não diretamente envolvida na investigação subjacente, o governo interpretou o caso da *Companhia Telefônica de NY* como uma autorização para que terceiros sejam demandados a cooperar com investigações criminais, contanto que (1) eles não estejam *muito* longe da matéria em questão, (2) a sua ajuda seja absolutamente necessária, e (3) a assistência técnica exigida não seja indevidamente onerosa.

Todas as vezes em que o governo federal pediu a um juiz para emitir uma ordem de desbloqueio, eles apresentavam a mesma manifestação em apoio ao pedido. Esta manifestação

tinha 1 parágrafo sobre o AWA e a *Companhia Telefônica de NY* e uma frase de análise jurídica que dizia que o caso *Companhia Telefônica de NY* dava à corte a autoridade para emitir a ordem solicitada à Apple. É isso. 1 parágrafo. Uma frase.

E até o início de outubro de 2015, os juízes rotineiramente aceitavam as ordens propostas pelo governo, sem nem emitir uma opinião analisando a questão. No total, o governo conseguiu pelo menos 70 ordens de desbloqueio emitidas à Apple por juízes federais pelo país. De acordo com o governo, a Apple nunca contestou nenhuma dessas ordens.

O CASO DO IPHONE DE NOVA YORK

Então, com a linguagem de formulário da Apple, a manifestação-padrão do governo, e juízes autorizando sem questionar, a máquina de ordens de desbloqueio para iPhones pré-iOS 8 estava funcionando tranquilamente, mesmo enquanto Comey publicamente lidava com a criptografia avançada no iOS 8 e depois no iOS 9.

No começo de outubro de 2015, um ano após a Apple anunciar o iOS 8, um juiz em Nova York chamado James Orenstein recebeu um pedido do governo para uma ordem com base no AWA direcionado à Apple para o desbloqueio de um iPhone. O juiz Orenstein tinha um histórico de recuar quando o governo argumentava por uma interpretação muito ampla da autoridade do AWA. Então, quando ele recebeu esse pedido de desbloqueio de iPhone, o juiz Orenstein não simplesmente o autorizou sob segredo de justiça, como muitos outros juízes antes dele. Ele emitiu uma decisão *fora de sigilo* recusando a concessão do pedido até que ele ouvisse a Apple.[4] Mas ainda que ele ainda não tivesse

4. [Nota da editora] UNITED STATES DISTRICT COURT EASTERN DISTRICT OF NEW YORK. *In Re Order Requiring Apple, Inc. To Assist In The Execution Of A Search Warrant Issued By This Court*. Juiz James Orenstein, julg. 9 de outubro de 2015. Disponível em: goo.gl/gyKqwm

decidido se daria provimento ao pedido de desbloqueio, a sua ordem de outubro mostrou como ele pensava sobre os problemas jurídicos envolvidos, e ela indicava o caminho para a sua decisão final sobre o pedido.

A ordem do juiz Orenstein rejeitou o argumento do Departamento de Defesa sobre o AWA. Ele argumentou que a lei, que é um estatuto preenchedor de lacunas [*gap-filling statute*], não pode dar ao governo a "autoridade que o Congresso optou por não conferir". Ele disse que, ao aprovar o CALEA, o Congresso não escolheu autorizar autoridades de investigação a compelir provedores a decifrar aparelhos. Ele distinguiu o caso da *Companhia Telefônica de NY* de diversas maneiras:

- < / > O status da Apple como empresa privada, não como [empresa de] utilidade pública altamente regulada, o que significa que ela é "livre para escolher a promoção do interesse de seus usuários em privacidade sobre o interesse concorrente das autoridades de investigação";
- < / > A existência de meios legais alternativos para obter a informação procurada, o que significa que a ordem de desbloqueio não era estritamente necessária;
- < / > A habilidade questionável dos tribunais de ordenar que a Apple destravasse um dispositivo que ela fabricou, porém de que ela não é dona; e
- < / > A falha do Congresso em mostrar qualquer intenção para forçar a Apple a fornecer a assistência às autoridades de investigação, apesar dos esforços do FBI, que eu mencionei, para expandir o CALEA.

No fim das contas, o fator-chave na análise do juiz Orenstein foi a questão do ônus da Apple para desbloquear o dispositivo em questão. Além disso, ele pareceu cético sobre a necessidade de forçar a Apple a – como ele colocou – "fazer o seu trabalho por você", considerando a existência de ferramentas forenses que o FBI possui para invadir iPhones, até os com iOS 8.

Depois de uma longa manifestação e uma audiência de duas horas, o juiz Orenstein decidiu o pedido de desbloqueio no final de fevereiro de 2016.[5] Ele emitiu uma decisão mordaz de 50 páginas negando o pedido de destravamento do governo. Ele demoliu totalmente a argumentação do *All Writs Act* avançada pelo governo, repetidamente a chamando de "absurda". Ele concluiu que não é "de acordo com os usos e princípios da lei" (a linguagem do AWA) "obrigar a Apple – uma parte privada com nenhum envolvimento em atividades criminosas [do réu] – a fazer um trabalho para o Estado contra sua vontade".

5. [Nota da editora] UNITED STATES DISTRICT COURT EASTERN DISTRICT OF NEW YORK. *In Re Order Requiring Apple, Inc. To Assist In The Execution Of A Search Warrant Issued By This Court*. Juiz James Orenstein, julg. 29 de fevereiro de 2016. Disponível em: goo.gl/57kTbZ

Orenstein se manteve coerente com sua análise sobre o CALEA do outubro anterior. Com o CALEA, ele deliberou, o Congresso havia considerado e declinado a adoção de uma lei que determinasse a assistência técnica aqui procurada, incluindo qualquer compulsão para colocar um *backdoor* nos produtos da Apple. Essas exceções no CALEA, as que foram tão duramente vencidas nas Guerras de Criptografia dos anos 1990, se provaram absolutamente fundamentais aqui. O Congresso, ele disse, sabe como requerer a assistência técnica de provedores quando quer: ele o fez no *Pen/Trap Act* e no *Wiretap Act*. Então, ele concluiu, o silêncio do Congresso nesse contexto em particular era uma escolha legislativa que não poderia ser contornada usando o AWA. O juiz castigou o governo por tentar fazer um desvio do processo legislativo por usar os tribunais para conseguir o que ele queria.

O juiz Orenstein havia forçado tanto a Apple quanto o Departamento de Justiça a trazer argumentos reais sobre o AWA. Ele fez o governo trazer algo além do seu único parágrafo padrão de jurisprudência e única frase de análise para tentar justificar seu argumento por uma interpretação

expansiva do AWA. Ele também forçou a Apple a tomar uma posição sobre a prática com a qual ela silenciosamente havia concordado por anos.

APPLE VS. FBI: O CASO DO IPHONE DE SAN BERNARDINO

Aqui é onde eu quero me voltar ao caso Apple vs. FBI: no começo de dezembro/2015, um ataque terrorista aconteceu em San Bernardino, Califórnia. Um homem e sua esposa mataram alguns de seus colegas de trabalho numa festa de fim de ano. Posteriormente, eles foram mortos pela polícia. Após sua morte, a polícia encontrou o iPhone do homem, que estava bloqueado, e apesar de conseguirem o mandado, o dispositivo estava com o iOS 9, o que significa que a Apple não poderia desbloqueá-lo para as autoridades. E como a polícia havia matado o atirador, não havia nenhuma pessoa viva que soubesse a senha.

Isso criou uma oportunidade inigualável para agentes de segurança avançarem sua pauta do "Going Dark". Não importava que, como o próprio diretor do FBI havia afirmado, criminosos determinados e sofisticados sempre irão encontrar formas de criptografar suas comunicações e seus dados. Não importava que os atiradores de San Bernardino mataram pessoas usando armas, e não smartphones. A ideia do terrorismo fornecia a racionalização perfeita para que as autoridades tentassem pegar de volta o poder perdido quando a Apple introduziu o iOS 8.

É bem parecido com a força que a corrupção tem para tentar mudar leis sobre vigilância e acesso das autoridades a dados no Brasil. Tem o mesmo tipo de gravidade, como vocês tem com a corrupção. Mas este uso covarde de uma calamidade nacional pela polícia não foi a novidade. Nós

sabíamos que eles iriam fazer isso porque a imprensa havia recentemente publicado, no verão anterior, um e-mail vazado que havia sido enviado por um dos principais advogados da comunidade de inteligência. No e-mail, ele disse que o ambiente legislativo não era muito amigável com uma lei de *backdoor*, mas que o ambiente "poderia se tornar" *anti-criptografia* "no evento de um ataque terrorista ou evento criminoso em que a criptografia forte tenha atrapalhado as autoridades". Então, poucos meses depois deste e-mail ter vazado, ocorreu o ataque em San Bernardino, que à época foi o pior ataque terrorista desde o 11 de setembro. Numa tentativa de aproveitar a oportunidade, o FBI foi aos tribunais para tentar obrigar a Apple a ajudá-los.

Para aproveitar ao máximo a oportunidade, o FBI foi à justiça para tentar forçar a Apple a ajudar. E, diferentemente das dezenas de casos de desbloqueio de iPhones que eles haviam levado anteriormente, eles não registraram o caso em segredo. Eles o registraram publicamente – uma ação que acabaria por contra-atacá-los no final.

Em 16 de fevereiro de 2016, passados mais de dois meses de investigação, o FBI obteve uma ordem via o AWA contra a Apple de um juiz em Riverdale, Califórnia, que fica próxima a San Bernardino. Assim como as outras ordens que o governo havia conseguido que tribunais emitissem contra a Apple para iPhones pré-iOS 8, essa ordem citava o *All Writs Act*, e ela mandava a Apple providenciar assistência técnica para o FBI para ajudá-los a acessar o telefone. Mas essa ordem, para um aparelho com iOS 9, era fundamentalmente diferente de qualquer outra ordem para desbloqueio de telefone que já havia sido vista. Ela ia muito, muito mais longe com o que era exigido à Apple.

O FBI queria que a Apple tornasse mais fácil para a agência tentar adivinhar à força bruta a senha. Para esse fim, a

/ CRIPTOGRAFIA É O NOVO CAPÍTULO NA HISTÓRIA DO DESCONFORTO DE AUTORIDADES COM TECNOLOGIAS QUE PERMITEM EXERCÍCIO DE DIREITOS HUMANOS. /

/ CRIPTOGRAFIA É APENAS MATEMÁTICA. ELA NÃO FUNCIONA DE UMA MANEIRA PARA A POLÍCIA E PESSOAS INOCENTES, E DE OUTRA PARA CRIMINOSOS. /

ordem mandava a Apple criar e criptograficamente assinar uma versão especial e debilitada do iOS que desabilitava certos recursos de segurança do iOS 9:

< 01 > Um limite de 10 tentativas erradas de adivinhar a senha, depois das quais o telefone trava e não te deixa adivinhar mais. Adicionalmente, se esse recurso opcional estiver ligado, o telefone apaga todos os seus dados após 10 tentativas erradas. O FBI não sabia se essa opção estava ligada.

< 02 > Uma demora gradativa entre tentativas, com a intenção de retardar os atacantes.

< 03 > Fazer com que o usuário digite manualmente a senha no telefone, ao passo que o FBI queria conectar o dispositivo a um computador que irá testar todas as combinações de senhas o mais rápido o possível.

Para ser clara, nada disso envolve mexer com a criptografia no telefone. A Apple não pode decifrar o aparelho, e o FBI não está tentando requerer o impossível. Essa ordem é integralmente sobre tentar adivinhar à força bruta a senha o mais rápido o possível. Mas isso exige que a Apple remova recursos que ela havia implementado para evitar com que as pessoas fizessem exatamente isso. Isso acontece porque, para a maioria dos usuários de iPhones, o motivo pelo qual eles colocam uma senha nos seus telefones é para manter os seus dispositivos seguros de assaltantes, hackers, parceiros abusivos, ou outros bisbilhoteiros. Alguém com más intenções que tome posse do telefone poderia tentar adivinhar a senha e acessar o aparelho. A Apple colocou esses três recursos para evitar que atores maus como estes o façam.

Em seu pedido para essa ordem sem precedentes, o governo pintou a ordem como modesta. É só esse único telefone, dessa única vez, eles disseram. É preciso ajudar a investigar um horrível ataque terrorista. E não é oneroso sob a AWA. A

Apple fez o iOS; ela faz softwares o tempo todo, então não é uma grande coisa escrever um pouco mais de software.

Mas a ordem que eles criaram, e a qual o juiz assinou, não tinha nada de modesta. Esse caso representou uma enorme mudança na estratégia do *All Writs Act* do governo. O governo norte-americano não estava apenas tentando forçar a Apple a fazer algo que a companhia já conseguia realizar, e que estava fazendo voluntariamente para as autoridades de investigação – nominalmente, contornando a senha em dispositivos rodando versões mais antigas do iOS. Isso já era ruim o suficiente, e já ia contra o AWA. Mas essa ordem ia ainda mais longe, esticando o AWA muito mais longe para forçar a Apple a criar, e tão importante quanto, registrar um iOS inteiramente novo que não existe no presente.

A argumentação do governo sobre o *All Writs Act* não colocava nenhum limite no que o AWA poderia permitir a um tribunal ordenar que um terceiro como a Apple fizesse. Sob esse raciocínio, a Apple, outros fabricantes de smartphones, e fabricantes de "Internet das Coisas" como smart TVs, todos poderiam ser forçados a transformar seus produtos em dispositivos de vigilância para autoridades de investigação. Nada no *All Writs Act* ou no caso da *Companhia Telefônica de NY* permite que terceiros sejam forçados a fazer serviços para autoridades de investigação dessa maneira. O AWA não permite que tribunais recrutem terceiros privados para fazer o trabalho da polícia por eles. A lógica do governo nos leva a um resultado extremo – a apropriação de nossos dispositivos para finalidades de vigilância.

Além disso, pelas razões que o juiz Orenstein explicou, a ordem estava diretamente em discordância com o CALEA. Quando o Congresso aprovou o CALEA, eles escolheram não conferir autoridade para os tribunais ou para as autoridades de investigação para forçar a ajuda que o FBI estava procu-

rando em San Bernardino. O governo não pode usar o AWA para conseguir algo que o Congresso reteve. Em suma, o poder do governo simplesmente não vai tão longe quanto o FBI afirmou que iria.

Não apenas a ordem original da corte era *juridicamente* errada, mas ela também levantou problemas significativos tanto da segurança de computadores, quanto de segurança pública de maneira geral. O governo argumentou que queria que a Apple criasse esse código para apenas um único telefone, apenas dessa única vez. Mas de maneira alguma ele teria mantido essa promessa. Nós sabemos de experiências passadas que quando autoridades de investigação pedem uma autorização judicial para usar novas técnicas de vigilância, eles justificam o pedido afirmando que irão utilizar a técnica para investigar crimes sérios, mas então eles acabam por usar esse método de vigilância para investigar crimes bem menos importantes. Isso iria acontecer aqui também. Além disso, o código iOS personalizado poderia ser utilizado abusivamente pela polícia para monitorar ativistas políticos ou espionar suas ex-namoradas.

E governos fora dos Estados Unidos, como o do Brasil, também iriam querer que a Apple criasse esse código especial para aplicar suas próprias leis. Mas muitos países têm leis que são inconsistentes com as liberdades civis e os direitos fundamentais humanos – como ser gay, insultar o Rei, ou seguir uma religião que não é sancionada pelo estado. São essas pessoas que acabariam se tornando os alvos de uma ordem de um governo estrangeiro para a Apple. Isso começa com investigar um telefone de um terrorista morto nos Estados Unidos e acaba com forçar a Apple a ajudar governos autoritários a perseguir seus cidadãos.

O medo das pessoas de seus governos leva a outro risco de segurança. Se a ordem judicial tivesse sido mantida, usuários de smartphones nos Estados Unidos e em outros lugares po-

deriam acreditar que seus governos têm a habilidade de forçar desenvolvedores de sistemas operacionais para celular a empurrar atualizações de software para seus telefones que iriam permitir que o governo acesse seus dados. Esse medo poderia levar pessoas a pararem de instalar atualizações automáticas de software, que são cruciais para a segurança geral do ecossistema da segurança de computadores. Essas atualizações de software consertam falhas de segurança *reais*, e atualizações automáticas garantem que os sistemas fiquem reparados sem que os usuários tenham que pensar muito sobre isso. Mas se as pessoas parassem de automaticamente atualizar seus dispositivos por medo, esses dispositivos desatualizados seriam hackeados, e eles iriam espalhar a infecção para outros aparelhos. Ou seja, o *medo* de ser hackeado pelo governo levaria muita gente a ser *realmente* hackeada por criminosos cibernéticos.

Outro risco ainda seria o de que o código iOS customizado escapasse das mãos da Apple ou das autoridades de investigação. Um código que poderia ser modificado para contornar o código de qualquer iPhone, não apenas do iPhone do alvo de uma investigação, seria um alvo atrativo para roubar, ou para subornar um oficial corrupto a vender. Ele poderia cair nas mãos de hackers e criminosos cibernéticos. Isso não é apenas uma especulação sem fundamentos. Diversos graves "hackeamentos" [*hacks*] e vazamentos de dados em agências federais americanas vêm acontecendo, incluindo o arsenal de ferramentas de hackeamento usado pelas nossas agências de inteligência. Nós sabemos que os governos não são tão bons em manter dados seguros.

O fato de que o governo estadunidense possui ferramentas à sua disposição para hackear dispositivos eletrônicos acabou sendo a coisa que encerrou o caso "Apple vs. FBI". Depois da ordem judicial original emitida em 16 de fevereiro, nós tivemos algumas semanas extremamente ocupadas. Du-

rante esse período, o caso virou manchete nacional. A Apple protocolou uma manifestação dizendo ao tribunal por que a ordem era onerosa e juridicamente imprópria. E por volta de 20 diferentes *amici curiae* foram protocolados por um número de pessoas e organizações (incluindo um que eu co-escrevi), a maioria em apoio à Apple, dizendo à corte as várias razões pelas quais a ordem era uma péssima ideia. O tribunal estabeleceu a data da audiência para o final de março de 2016.

E então, um dia antes da audiência, o governo notificou a corte de que possuía uma ferramenta forense de terceiros que talvez o deixasse ter acesso ao telefone. A audiência foi adiada. Alguns dias depois, o governo confirmou que ele havia conseguido acessar o telefone usando essa ferramenta não identificada que ele havia comprado de um terceiro, supostamente por centenas de milhares de dólares. Agora que ele tinha acesso ao telefone, não precisava mais da ajuda da Apple. Então o governo largou o caso, e a corte suspendeu a sua ordem de 16 de fevereiro. A Apple não teve que fazer o código iOS customizado.

Esse é um final feliz, mas que deixa muitas questões sem resposta. Nós ainda não sabemos como o governo acessou o telefone. Ele nunca falou para a Apple ou para o público qual era a ferramenta, ou quem a fabricou, ou qual vulnerabilidade no iOS ela explorou. Então isso continua um mistério, e isso significa que há um ponto fraco no iOS que pode não ter sido reparado.

E nós não sabemos qual é a abrangência do *All Writs Act*. O tribunal nunca conduziu nenhuma análise jurídica sobre se era apropriado emitir aquela incrivelmente perigosa ordem para a Apple. Nós não sabemos quais tipos de ônus a corte pode levar em consideração ao avaliar se uma ordem para uma companhia de terceiros como a Apple é muito onerosa para passar sob o AWA. Nós também não sabemos se os tribunais podem

adequadamente levar interesses exteriores em consideração quando eles estão conduzindo uma análise sob o AWA. Como eu expliquei, a ordem para a Apple teria amplas consequências para a segurança dos computadores, assim como implicações internacionais para os direitos humanos. A corte pode levar esses interesses para sua análise, ou ela tem que ignorá-los?

Tem que existir alguma limitação para o que atores privados podem ser ordenados a fazer sob o AWA, mas por causa da maneira como esse caso terminou, nós não sabemos onde estão esses limites. O governo cancelou a audiência no último minuto, então eles não tiveram seus argumentos absurdos sobre a AWA testados em um tribunal aberto. Lembrem-se, o governo vê tudo o que é requisitado como preservação do *status quo* em que ele espera ter o total direito de acesso a dados. Ou seja, o governo acredita que não deve existir uma caixa que não possa ser aberta, nenhuma comunicação que não possa ser interceptada.

Preocupantemente, as autoridades de investigação dos Estados Unidos têm mostrado que estão dispostas a sacrificar a segurança de todos para viver nesse mundo, ainda que uma segurança robusta via criptografia também *previna* crimes. E porque os agentes partem de uma posição de poder limitado sob a Constituição dos Estados Unidos, o incentivo deles é constantemente procurar a expansão desse poder, mesmo que em suas mentes, eles estejam apenas preservando o *status quo*.

Isso me faz pensar que o governo não vai deixar a sua derrota vergonhosa no caso "Apple vs. FBI" o desencorajar de continuar a usar os tribunais para conseguir mais e mais poder pela expansão do AWA. O governo pode continuar a trazer outros casos em outros tribunais a outros juízes, até que ele consiga outra ordem, como a original no caso da Califórnia, que o dá o que ele quer. Então ele pode usar *essa* ordem para

persuadir *ainda mais* tribunais de que é apropriado emitir esse tipo de ordem.

E é quase certo que ele irá atrás dessas ordens expansivas do AWA sob sigilo daqui para frente. A escolha do governo em protocolar o caso "Apple vs. FBI" publicamente acabou se revelando um grande erro, porque embora o caso envolva um horrível ataque terrorista, a opinião pública majoritariamente ficou do lado da Apple. O governo não irá cometer esse erro de novo.

Na verdade, até onde sabemos, nos 14 meses desde que o caso Apple vs. FBI se encerrou, ele pode já ter conseguido ordens de assistência técnica sob sigilo que forcem a Apple ou alguma outra companhia a fazer o que a Apple teria que ter feito nesse caso – ou pior. Pode existir todo um corpo de direito secreto sobre o qual nós não sabemos, feito sob sigilo, obrigando fabricantes de smartphones ou provedores de serviços de e-mail ou fabricantes de aplicativos de mensagens a contornar a criptografia para agentes de segurança na aplicação da lei de um jeito ou de outro.

Mesmo que outras cortes rejeitem as futuras tentativas do governo para abusar do AWA, o governo pode usar essa rejeição para sua vantagem, também. Se os tribunais continuarem a determinar que o AWA não permite o que o FBI deseja, o FBI pode argumentar para o Congresso que existe a necessidade de uma nova lei que *sim* o permita. Lembrem-se, a estratégia do "Going Dark" possui vários tentáculos – não apenas os tribunais, mas legislativos e pressões privadas em empresas. Se um não funcionar, o governo pode pressionar outro. E enquanto eles acreditarem que "manter o *status quo*" de seu poder significa lutar para manter e até expandir as suas capacidades de vigilância, não importa a qual custo para a privacidade humana ou agência ou computador e até segurança física, nós devemos esperar que eles continuem pressionando.

E O BRASIL?

Isso me leva aos casos do WhatsApp aqui no Brasil. Eu gostaria de encerrar com algumas observações sobre as dinâmicas do poder que entram em jogo nesses casos. Algumas delas são iguais às que estão em questão no debate sobre criptografia nos Estados Unidos. Mas há um outro aspecto delas com o qual vocês provavelmente já estão bem familiarizados, mas que não entra em jogo no debate americano.

Como vocês sabem, o WhatsApp foi bloqueado em todo o país várias vezes, cada uma delas pela ordem de um único juiz em um único tribunal, por falhar em cumprir solicitações da justiça para dados relevantes em investigações criminais. Esses bloqueios afetaram 100 milhões de pessoas, ou quase a metade da população brasileira. Esse é um impacto no mundo real surpreendentemente amplo baseado em apenas um dos vários mandados judiciais para dados de usuários que são emitidos todos os anos para várias empresas de Internet, incluindo o WhatsApp.

Esses bloqueios foram revertidos ou cancelados porque bloquear o acesso de 100 milhões de pessoas é claramente fora de proporção com o que o WhatsApp fez. A prisão de um executivo do Facebook na ordem do juiz de Sergipe que emitiu a segunda ordem de bloqueio também foi uma medida extremamente agressiva a se tomar em resposta ao não cumprimento de uma ordem judicial em um único caso. Mas para mim, a desproporcionalidade dessas respostas ao não cumprimento do WhatsApp parece ser parte do ponto. Prender o oficial de uma empresa e ordenar que o serviço ficasse bloqueado em todo o país por vários dias foi uma maneira de mostrar poder por parte desses juízes depois que o não cumprimento do WhatsApp os fez se sentir sem poder.

Por que eles se sentiram sem poder? Porque o WhatsApp se negou a entregar dados, aparentemente incluindo o con-

teúdo de mensagens de WhatsApp. O WhatsApp *não poderia* produzir essas mensagens, nem se o quisesse e nem se a lei dos Estados Unidos potencialmente não o proibisse de fazê-lo. Isso acontece porque as mensagens de WhatsApp são criptografadas de ponta-a-ponta, o que significa que nem a própria empresa pode ler as mensagens ou fornecê-las de uma forma legível para a polícia. Isso é o que fez o bloqueio e a prisão parecerem tão injustos para qualquer um que entendia a tecnologia de criptografia envolvida: o WhatsApp estava sendo punido por não cumprir ordens que eram *impossíveis* de serem cumpridas pelo WhatsApp. É como algo de um livro do Kafka.

Só para afirmar, não é como se não houvesse nenhum precedente histórico de provas que sejam *impossíveis* de obter para investigadores. É sempre o caso que alguma informação estará permanentemente além do alcance das autoridades de investigação e dos tribunais. Conversas tidas em pessoa geralmente não são gravadas. Documentos se perdem ou são destruídos antes de virarem relevantes para uma investigação. Testemunhas esquecem coisas, ou morrem, ou não são encontradas. Não há nada que o Estado possa fazer sobre isso sem um estado de vigilância Orwelliana tão integral, tão invasivo, que a privacidade e a agência humana seriam impossíveis.

Mas nós não estamos lá. Ainda não. Nós estamos aqui, e no presente momento, tribunais e autoridades de investigação estão sofrendo para absorver o impacto da criptografia em investigações criminais. Claro que um juiz não vai mandar prender alguém porque a sua empresa se recusa a entregar gravações inexistentes de conversas que nunca nem foram gravadas, pra começar. É impossível produzir provas que nunca existiram, e isso é fácil para um juiz compreender. Mas com a criptografia de ponta-a-ponta para comunicações

escritas, ele sabe que a evidência existe, e ainda assim ele é informado de que não é possível obtê-las pelos meios usuais, como mandados de busca ou grampos. Esse é um *novo tipo* de "impossibilidade", e para a polícia e juízes por muito tempo acostumados com possuir um grande poder, pode ser muito difícil compreender ou aceitar.

Portanto nós podemos entender a resposta de juízes que bloquearam o WhatsApp e mandaram prender um funcionário do Facebook. Foi uma demonstração desses juízes do *velho* e *tradicional* tipo de poder. Como eu disse no início, o Estado está acostumado a ter todo o poder. E o poder máximo do Estado é a coerção. Ele pode ordenar que todas as empresas de telecomunicações em todo o país bloqueiem um serviço, pensando que o serviço então irá ceder e fazer o que o Estado deseja. Na mesma teoria, ele pode tentar forçar obediência ao prender alguém no seu caminho para o trabalho e colocá-lo na prisão. Mas quando a obediência *simplesmente não é possível*, nem a coerção funciona.

Mas o problema para as autoridades brasileiras nos casos de WhatsApp não é só que a criptografia de ponta-a-ponta torna impossível para a companhia reproduzir os conteúdos de mensagens de WhatsApp para autoridades de investigação de uma maneira legível. Esses casos são também sobre os desafios que os países enfrentam quando tentam aplicar suas leis contra companhias que têm sede nos Estados Unidos e operam mundialmente.

Meu colega Greg Nojeim falará com vocês em breve sobre os problemas de pedidos transfronteiriços de dados [*cross-border data demands*]. Eu não vou atropelá-lo, mas eu gostaria de trazer à tona outra dinâmica do poder em jogo nos casos do WhatsApp. Os Estados Unidos são um superpoder dominante no cenário mundial. E eles usam esse poder de maneiras que muitas vezes os fazem serem vistos

como arrogantes e ignorantes das necessidades e valores de outras sociedades.

Essa dinâmica de poder, e a tensão que a acompanha, se espalham para os relacionamentos que as empresas de tecnologia estadunidenses têm com outros países em que elas têm usuários. As empresas têm dados desses usuários. Investigadores em outros países querem esses dados, e eles estão acostumados a ter o poder de conseguir o que eles querem. Mas nos casos de bloqueio do WhatsApp, a empresa respondeu a essas demandas de dados de usuários asseverando três diferentes limites de poder: (1) que ela não possui o poder de entregar os conteúdos de mensagens de WhatsApp, porque elas estão cifradas de ponta-a-ponta; (2) que o direito estadunidense limita o poder do WhatsApp para liberar essa informação, ainda que eles tivessem a habilidade de fazê-lo – ou seja, o direito estadunidense é mais poderoso do que o direito brasileiro; e (3) que existem limites jurisdicionais no poder dos tribunais brasileiros para exigir esses dados de uma empresa americana.

Como esperado, essa resposta não foi bem recebida. No caso do terceiro bloqueio de WhatsApp, a juíza Daniela Barbosa, do Rio, ordenou que o WhatsApp "desabilite a chave de criptografia", ou até que realize o que é chamado de ataque do "homem do meio" ["*man in the middle" attack* - MITM], para que assim fosse possível interceptar os conteúdos de mensagens de WhatsApp de uma maneira legível. Vamos deixar de lado a questão de se essas coisas são *tecnicamente* possíveis (embora ambas sejam uma má ideia). O que pareceu enraivecer a juíza Barbosa mais do que o não cumprimento do WhatsApp com os *termos* da ordem foi a *maneira* com a qual o WhatsApp respondeu à sua ordem: eles responderam com questões para a corte, as quais eles enviaram, via email, em inglês.

Aqui está como a juíza Daniela Barbosa reagiu a isso:

> "Ao ofício assinado por esta magistrada, contendo a ordem de quebra e interceptação telemáticas das mensagens do aplicativo Whatsapp, a referida empresa respondeu através de e-mail redigido em inglês, como se esta fosse a língua oficial deste país, em total desprezo às leis nacionais, inclusive porque se trata de empresa que possui estabelecida filial no Brasil e, portanto, sujeita às leis e à língua nacional, tratando o país como uma 'republiqueta' com a qual parece estar acostumada a tratar."[6]

6. [Nota da editora] PODER JUDICIÁRIO DO RIO DE JANEIRO. 2ª Vara Criminal de Duque de Caxias. Inquérito Policial 062-00164/2016. Juíza Daniela Barbosa Assumpção de Souza, julg. 19 julho de 2016. Disponível em: goo.gl/XLfoip

Bom, me desculpem, a minha pronúncia de português é horrível. Mas eu queria lê-la ao invés da versão em inglês de propósito. Para que então vocês possam relacionar como vocês se sentiram ao me ouvir assassinar a sua maravilhosa língua a como a juíza Barbosa deve ter se sentido quando o WhatsApp enviou seu email em inglês para questionar a sua ordem.

A maneira na qual as empresas de tecnologia estadunidenses se comportam pode parecer tão arrogante quanto o governo estadunidense parece quando demonstra seu poder. Particularmente no Brasil, esse tipo de demonstração de poder por empresas dos Estados Unidos, desafiando o poder das instituições brasileiras, pode ser visto como uma reencarnação das dinâmicas de poder coloniais e imperialistas que o Brasil passou sua vida inteira como país independente tentando superar. As empresas estadunidenses não estão apenas resistindo à jurisdição de agentes de segurança pública de outros países, mas também, as autoridades de investigação estadunidenses agora têm autoridade, sob as leis de procedimentos criminais americanas, para hackear computadores em qualquer lugar do mundo ao executar um mandado de busca, sob certas

circunstâncias. E ainda assim, aqui está uma companhia norte-americana dizendo às autoridades de investigação e tribunais do Brasil que eles não podem adentrar os Estados Unidos para forçar o WhatsApp a cumprir uma ordem judicial.

É compreensível, então, que os tribunais brasileiros tenham respondido ao comportamento de companhias de Internet estadunidenses exercendo maneiras tradicionais de poder, como bloquear um serviço ou prender alguém. Os requerimentos de localização de dados no Marco Civil também são uma afirmação do poder tradicional, em resposta às queixas de autoridades estadunidenses de limites jurisdicionais à sua autoridade.

Agora isso parece uma luta pelo poder não entre a polícia e o povo, como eu falei no início, em que indivíduos usam novas tecnologias para nivelar o jogo entre eles e o Estado. Parece uma luta pelo poder em um nível geopolítico. E batalhas geopolíticas têm uma tendência lamentável de deixar de fora os interesses dos indivíduos humanos reais que são afetados.

É isso que os tribunais que *anularam* as ordens de bloqueio reconheceram: a demonstração de poder tradicional ao bloquear o WhatsApp causou danos colaterais para milhões e milhões de brasileiros. Os juízes que emitiram as ordens de bloqueio estavam dispostos a sacrificar os interesses de *metade da população do país* para mostrar ao WhatsApp quem estava no comando. A juíza Barbosa, que ordenou que o WhatsApp "removesse a chave de criptografia" e iniciasse um ataque MITM, estava disposta a ordenar que o WhatsApp comprometesse a segurança de seu serviço – o que poderia ter afetado a segurança de *todos* os usuários de WhatsApp – para que fosse possível coletar provas em apenas um caso. Isso é semelhante ao Apple vs. FBI, quando o FBI estava disposto a enfraquecer a segurança de *todos* os usuários de iPhone, e até a segurança física de usuários localizados em países autoritários, para ter acesso a apenas um telefone.

Nem o juiz do caso Apple vs. FBI, nem os juízes que emitiram as ordens de bloqueio do WhatsApp pareceram entender que essas seriam as graves consequências de suas ações. Ao invés disso, na batalha entre o poder do Estado e o poder da criptografia, os usuários médios que não fizeram nada de errado foram pegos no fogo cruzado.

Quando o Supremo Tribunal Federal avaliar os casos de bloqueio de WhatsApp nos próximos dias, pode haver uma tentação de interpretar o Marco Civil de uma maneira que permita o exercício do poder de bloqueio sob uma empresa estadunidense que tem sido vista como intransigente. O artigo 11 do Marco Civil diz que a lei brasileira "deve ser obrigatoriamente respeitada".[7] Mas é importante que os ministros reconheçam que defender as leis do BRASIL não deve significar sacrificar o interesse de BRASILEIROS. Privacidade, liberdade de expressão e segurança são direitos fundamentais, e a criptografia ajuda a protegê-los. Isso é algo que a polícia e os tribunais em todo o país deveriam acolher. É importante que a lei – seja o Marco Civil aqui no Brasil, ou o *All Writs Act* nos Estados Unidos – seja interpretada de maneira a respeitar os direitos fundamentais. Eu tenho a esperança de que o Supremo Tribunal Federal fará a coisa certa.

7. [Nota da editora] Lei Federal 12.965, de 23 de abril de 2014. Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

PERGUNTAS/RESPOSTAS

< PERGUNTA > Meu nome é Giovanna, eu sou aluna do curso de mestrado aqui da faculdade de direito, minha pergunta vai no sentido do que você estava falando, sobre essa questão de como são interpretadas essas recusas das empresas e como isso afeta até como a criptografia é enxergada.

Se não tem também um outro lado do argumento, que seria que as empresas estão querendo os dois lados da moeda. No sentido de que a criptografia se popularizou, nós consumidores temos acesso a ela, aparentemente, mas por outro lado, não tem muita certeza de para onde vão os dados da minha nuvem, para onde vão os dados do WhatsApp, como o meu histórico de busca do Google é comercializado, enfim. Parece que essa posição das empresas, uma hora defende nossa privacidade, uma hora vende tudo, e nós ficamos no meio dessa guerra. Então, como isso também afeta essa percepção da criptografia como algo favorável ao consumidor.

< RIANA > É uma boa pergunta. Eu concordo que, de um modo geral, as empresas americanas de tecnologias querem ser vistas como muito protetoras da privacidade de seus usuários, mas é claro que elas pensam que a lei americana deve governar esses dados. Nos EUA, nós não temos o padrão que se tem aqui e em outros países europeus, onde a presunção de uso comercial de dados de usuários é – nos EUA, permitido a não ser que expressamente proibido, enquanto no Brasil e Europa, o inverso, proibido a não ser que expressamente dito. Então, essa é a moldura que se tem: a lei americana permite esse uso dos dados, mas aqui as empresas têm de lidar com o Marco Civil, e na Europa, com outras leis que realmente mudam um cenário onde milhões de pessoas estão usando seu aplicativo.

Dito isso, eu acho que companhias como a Apple – sendo amigáveis à privacidade dos usuários – o fazem parcialmente por acreditarem nisso, e em parte como um esforço de relações públicas. Então, por exemplo, eu mencionei que haviam dezenas – 70 ou mais –de ordens para desbloquear iPhones com versões anteriores ao iOS 8, e a Apple nunca rejeitou nenhuma delas, tendo, na verdade, escrito a linguagem que estava nas ordens judiciais. E estava disponível em suas dire-

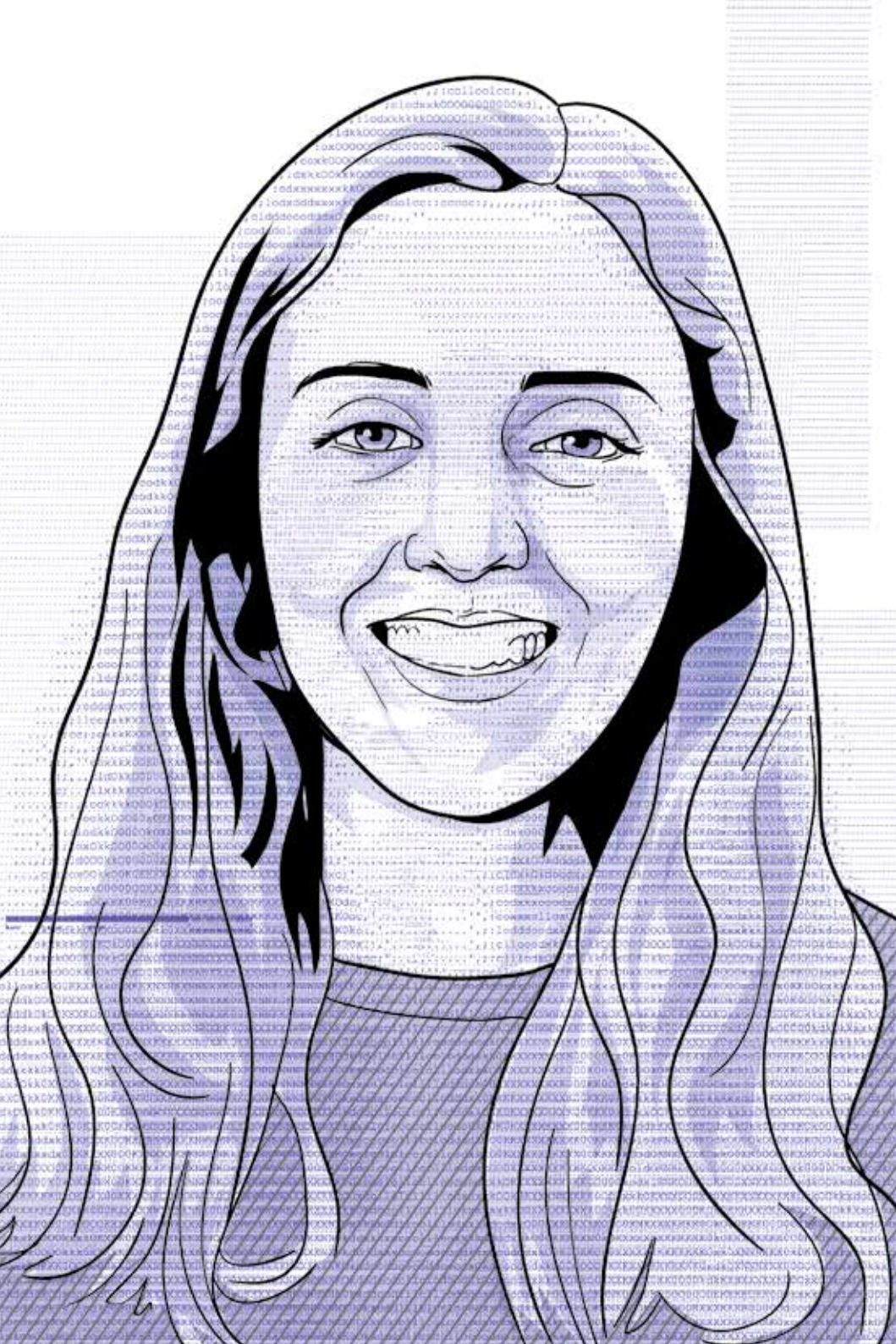
trizes para autoridades de investigação. Você quer conseguir uma ordem para desbloquear um iPhone pré-iOS 8? Bem, aqui está a linguagem que você precisa conseguir em uma ordem judicial, e então trazer à nós para fazermos o desbloqueio. Existem excelentes razões para fazerem isso, pois ao preparar a linguagem, eles possuem controle sobre o que podem ser forçados a fazer, para que os oficiais não retornem com novos pedidos não contemplados na ordem judicial. São boas razões. Mas quando esse fato veio a público, ou seja, após os primeiros casos judiciais envolvendo essas ordens, pode ter sido um pouco embaraçoso. Ao mesmo tempo que diziam estar tentando proteger a privacidade dos usuários usando a criptografia, estavam sendo complacentes ao escreverem eles mesmos [os termos d-] as ordens judiciais. Então, eu acredito que certamente existem dois lados. Mas quero enfatizar a estranha falta de um padrão de lei sobre privacidade que os EUA têm quando comparado a outros países, já que [nos EUA] tudo que não é proibido, é permitido.

< PERGUNTA > Vou ficar com o inglês. Meu nome é Dan, e sou da Universidade de Washington e do Instituto Igarapé. Estou curioso para que você fale sobre quais são, na sua opinião, as perspectivas para os EUA indo adiante, um assunto que você tocou brevemente. Mas gostaria de ouvir um pouco mais sobre o que você espera desse novo governo no tocante a essas questões. Presumo que não seja bom – essa é a minha perspectiva. Mas ao mesmo tempo, sinto que há bastante oposição também, bastante apoio de organizações como a ACLU e a EFF, que estão se mobilizando contra esses movimentos. Então, ao mesmo tempo acredito que existem oportunidades, sobre as quais gostaria de ouvir a sua visão.

< RIANA > Acho que concordo com a sua visão sobre isso. Penso que também houve um movimento durante o último governo para aprovar uma lei que protege a criptografia, se não

me engano são quatro congressistas com diplomas na área de ciência, tecnologia, engenharia ou matemática. De todo o Congresso, apenas quatro. Um deles apresentou um projeto de lei para tornar claro que as empresas não têm a obrigação de criar *backdoors* em seus produtos ou enfraquecer seus algoritmos de criptografia, incluindo as empresas de smartphones, e não só as empresas de telecomunicações submetidas ao CALEA. Ele acabou não indo para lugar nenhum. Mas também, como eu disse, as leis que obrigavam as empresas a fazerem isso também não foram a lugar nenhum. E o Congresso estava tão dividido e incapaz de fazer qualquer coisa naquele momento como está agora. Não gosto de confiar apenas em incompetência e problemas internos para impedi-los de fazer qualquer coisa. Não conseguiram até agora, e temos um partido controlando ambas as casas, então, se eles quiserem podemos ver uma nova tentativa de introduzir essa lei, mas ao mesmo tempo, não vemos esse nível de engajamento político do público norte-americano há muito tempo, certamente não durante meu tempo de vida. Organizações como a ACLU e a EFF continuarão lutando para limitar isso, mas honestamente, acho que agora o governo está muito distraído com muitas outras crises horríveis acontecendo, de modo que será difícil conseguir transformar essa tensão em algo como isso.

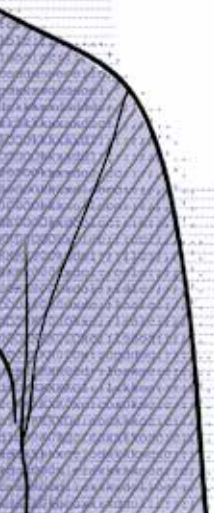
Dito isso, como disse o advogado da comunidade de inteligência no e-mail vazado, talvez aconteça algo que mude a maré. Fiquei muito feliz quando no caso "Apple vs. FBI" nada aconteceu, assim como no tiroteio da Pulsenight na Flórida. Não houve nenhum projeto de lei apresentado quando isso aconteceu. Pode ser que algo muito pior seja necessário, o que eu realmente espero que não aconteça, para fazer com que uma lei anti-criptografia vá para qualquer lugar, e mesmo assim, eu duvido que o Congresso seja capaz de fazer qualquer coisa. Então, acho que a resposta é ¯_(ツ)_/¯.



07.

OBTENÇÃO DE EVIDÊNCIAS DIGITAIS: QUANDO SÃO NECESSÁRIOS PEDIDOS DE COOPERAÇÃO INTERNACIONAL?

Jacqueline de Souza Abreu



A apresentação no congresso e este texto baseiam-se em ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. *Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais*. São Paulo: InternetLab, 2017, pp. 41-45. Disponível em: goo.gl/TQ7U8E

O ESTADO ATUAL DA DISCUSSÃO

Diversas autoridades brasileiras têm reivindicado o poder de solicitar diretamente de empresas estrangeiras como Google, Microsoft, Facebook e Yahoo dados relevantes para investigações. Por *diretamente*, quero dizer independentemente e fora de procedimentos de cooperação jurídica internacional (MLAT).

Ao lado desse argumento, há decisões históricas do Superior Tribunal de Justiça. O caso mais emblemático nessa temática é o do Inquérito nº 784/CF, de 2013, em que a Google Brasil Internet Ltda. impetrou mandado de segurança contra ofício da Polícia Federal pelo qual se requisitou a quebra de sigilo telemático de contas do *gmail*. A empresa alegou que (i) não tem acesso aos computadores que armazenam os dados; (ii) os computadores em que os dados estão armazenados estão nos Estados Unidos; (iii) os computadores são operados e os dados são detidos pela sua controladora, Google Inc., a qual está proibida de fornecer dados a autoridades estrangeiras fora da via diplomática (tratado bilateral de cooperação jurídica).

A ministra Laurita Vaz do Superior Tribunal de Justiça (STJ) rejeitou os argumentos apresentados pela Google Brasil, afirmando que "o fato de esses dados estarem armazenados em qualquer outra parte do mundo não os transforma em material de prova estrangeiro, a ensejar a necessidade da utilização de canais diplomáticos para transferência desses dados". Segundo observou, "o que se pretende é a entrega de mensagens remetidas e recebidas por brasileiros em território brasileiro, envolvendo supostos crimes submetidos induvidosamente à jurisdição brasileira". Também asseverou que "remeter o Poder Judiciário Brasileiro à via diplomática para obter dados é afrontar a soberania nacional, sujeitando o Poder Estatal à inaceitável tentativa da empresa em questão de se sobrepor às leis pátrias [...]". A Microsoft Informática Ltda. já desafiou ordens de quebra de sigilo de e-mails *hotmail* em termos se-

melhantes à Google Brasil e o resultado de derrota no STJ foi o mesmo.[1]

A questão não está, entretanto, pacificada nesse sentido em todos os tribunais. Em 2014, a Yahoo! do Brasil Internet Ltda. foi alvo de ação civil pública proposta pelo Ministério Público Federal (MPF) em razão dos alegados "reiterados descumprimentos de ordens judiciais" determinando o fornecimento de dados de usuários. Segundo argumentou o MPF[2], seria dever legal da empresa fornecer as informações requisitas, pois a empresa presta serviço no país, ainda que seus provedores estejam localizados no estrangeiro. "O que importa é se detém ou não a informação requisitada judicialmente", argumentou. Como a informação estaria sob total controle das sócias da Yahoo Brasil, domiciliadas nos EUA e com poder sobre a administração da empresa brasileira, haveria possibilidade de (forçar o) fornecimento. A Justiça Federal acolheu a argumentação de defesa, no sentido de que a Yahoo Brasil não tem obrigação de fornecer dados pertencentes a conta de e-mail criada junto a pessoa jurídica diversa (Yahoo! Inc., que administra as contas @yahoo.com). A Yahoo Brasil deve fornecer dados de usuários que efetivamente se cadastraram na versão brasileira do serviço de e-mail (@yahoo.com.br) e anuíram aos seus termos de uso. É o "provedor responsável", terminologia do Marco Civil da Internet, que tem a obrigação de disponibilizar.[3]

A tese da diferenciação entre subsidiária/encarregada de publicidade e matriz/operadora da plataforma também recentemente ajudou o Facebook. Em novembro de 2016, a Justiça Federal do Rio Grande do Sul decidiu que o Ministério Público Federal (MPF) deve obter conteúdo de comunicações privadas

1. SUPERIOR TRIBUNAL DE JUSTIÇA, Recurso em Mandado de Segurança nº 46.685/MT. Min. rel. Leopoldo de Arruda Raposo, julg. 26.03.2015.

2. MPF/SP pede condenação da Yahoo! Brasil por desobediência a ordens judiciais, JusBrasil, Procuradoria Geral da República. Disponível em: goo.gl/sZUmLc Acesso em: 19.01.2017.

3. JUSTIÇA FEDERAL. Processo nº 0012450-95.2014.403.6100. Juíza Federal Sílvia Figueiredo Marques, julg. 13.05.2015.

transmitidas na rede social Facebook pela via diplomática, uma vez que tais dados são controlados pela Facebook Inc. e/ou Facebook Ireland Limited.[4] A subsidiária brasileira Facebook Serviços Online do Brasil Ltda., que usualmente recebe as ordens judiciais com determinações de fornecimento de dados, vêm argumentando reiteradamente em diversos processos que apenas presta serviços relacionados a publicidade, não detendo informações relativas a usuários, e que, sempre que recebe requerimentos de autoridades brasileiros, encaminha-os para os efetivos operadores da rede social. Nos autos de Ação Civil Pública proposta pelo MPF contra a Facebook Brasil contra os mesmos "reiterados descumprimentos de ordem judicial", a empresa também acumula vitórias na primeira e na segunda instância da Justiça Federal, que indeferiram a ação por razões formais: falta de interesse de agir e impossibilidade do pedido.[5]

4. "MPF deve obter dados do Facebook nos EUA por tratado", Jota, 02 de dezembro de 2016, disponível em: goo.gl/ayhMJD Acesso em: 19.01.2017.

Mais recentemente, a discussão passou a envolver os termos do Marco Civil da Internet. Muitas autoridades citam o art. 11 do Marco Civil da Internet, que determina que provedores de conexão e aplicações de Internet respeitem a "legislação brasileira e os direitos à privacidade, à proteção de dados pessoais e ao sigilo das comunicações privadas e dos registros" "em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações em que pelo menos um desses atos ocorra em território nacional", como sustentação para o argumento de que o Brasil têm jurisdição sobre as empresas, fazendo com que pedidos via MLATs sejam desnecessários. A lei estabelece que

5. O processo nº 0013254-29.2015.4.03.6100 relativo à Ação Civil Pública proposta pelo MPF contra a Facebook Brasil pode ser acompanhado na plataforma Observatório do Marco Civil, em goo.gl/5X3T5t . A decisão mais recente do Tribunal Regional Federal da 3ª Região é de 20 de julho de 2016. Em 26 de janeiro de 2017, foi admitido recurso especial do MPF ao STJ.

/ AS ORIGENS DO IMPASSE ENTRE AUTORIDADES DE INVESTIGAÇÃO E EMPRESAS SEDIADAS NO EXTERIOR ESTÃO NO CONCEITO DE ‘JURISDIÇÃO’ /

/ UMA SAÍDA
É REFORMULAR
O MODELO DE
COOPERAÇÃO
JUDICIÁRIA
E REPENSAR
OS FATORES
DEFINIDORES DE
JURISDIÇÃO SOBRE
DADOS DIGITAIS. /

a obrigação de respeitar a legislação brasileira no tratamento de dados se aplica aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil (art. 11, §1º); e mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil (art. 11, § 2º). As empresas, por sua vez, citam o parágrafo único do art. 3 do Marco Civil, segundo o qual "os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte", caso dos MLATs.

ORIGENS DO PROBLEMA

Para entender as origens do impasse entre autoridades de investigação e empresas sediadas no exterior, para além dos termos legais do Marco Civil da Internet, é preciso ter em mente o conceito de "jurisdição", que, no direito internacional público, consiste basicamente na autoridade de exercer poder sobre pessoas e coisas em um determinado território.[6] Como um Estado detém jurisdição dentro de seus limites geográficos, tornou-se necessária a instrumentalização de meios de cooperação internacional para situações nas quais autoridades públicas de um Estado-nação esbarram nos limites de seu poder, como quando precisam extraditar suspeitos, ouvir testemunhas ou colher provas que se encontram no exterior.[7] Para este fim, são tradicionalmente utilizadas cartas rogatórias e celebrados acordos de cooperação mútua entre países, por exemplo.

6. Ver ACCIOLY, Hildebrando; SILVA, G. E. do Nascimento; CASELLA, Paulo Borba. *Manual de Direito Internacional Público*. 18ª Edição. São Paulo: Saraiva, 2010, p. 321.

7. SOUZA, Carolina Yumi de. "Cooperação jurídica internacional em matéria penal: considerações práticas", *RBCCRIM*, vol. 71, pp. 297-325, 2008, p. 300.

Esse modelo funcionou com sucesso – e, na maior parte das situações, ainda funciona –por duas razões centrais. Primeiro, porque, em geral, é um esquema idealizado para situações raras e excepcionais. Na grande maioria dos processos, não há que se realizar extradições, ouvir testemunhas estrangeiras nem obter provas no exterior. Segundo, porque a identificação dos limites da jurisdição e da necessidade de se recorrer a meios de cooperação é relativamente simples para meios físicos: se autoridades do país A precisam de pessoas ou documentos fisicamente localizados no território do país B, o país A necessariamente precisa solicitar cooperação do país B, já que não pode exercer poder fora de seu território.

A questão assumiu contornos mais complexos com a Internet. Primeiro, porque a necessidade de colheita de *provas digitais* armazenadas em computadores no exterior ou detidas por empresas sediadas no exterior se tornou uma atividade cotidiana. Segundo, porque "documentos digitais" (dados em geral como informações cadastrais, registros, conteúdo de comunicações), ao mesmo tempo em que de fato estão localizados em servidores físicos em (ao menos um) lugar certo, também podem ser acessados virtualmente de diversos lugares do mundo. Além disso, as "pessoas" que detém o controle sobre os servidores onde os dados estão armazenados e/ou sobre o acesso a eles, os provedores de aplicações de Internet, estão presentes multinacionalmente, seja por sedes e subsidiárias ou apenas virtualmente.

Quando se recusam a fornecer dados de usuários mediante direta requisição e/ou ordem de autoridade brasileira, fora dos trâmites dos acordos de cooperação internacional, empresas de Internet se baseiam nessas doutrinas clássicas a partir das quais se edificaram os limites jurisdicionais e a construção de acordos de cooperação mútua – os fatos de que os dados buscados como evidência digital estão fisica-

mente armazenados no exterior e/ou detidos por pessoa estrangeira. Não há nada de desafiador à soberania nacional quando assim o fazem; pelo contrário, o modelo de cooperação internacional foi pensado para conciliar o respeito a diferentes nações.

Apesar disso, a emergência de leis *extraterritoriais* ou pelo menos de interpretações *extraterritoriais* do escopo de obrigações de cooperação com autoridades estatais na entrega de dados de usuários tem colocado provedoras transnacionais de serviços de internet em situações complicadas, quando as diferentes legislações nacionais a que estão simultaneamente submetidas estão em conflito, isto é, quando obedecer a uma implica desrespeitar outra. É frequentemente este o caso do embate do Brasil com empresas norte-americanas, já que a legislação americana aplicável ao fornecimento de dados de usuários a autoridades proíbe provedores de entregar *conteúdo* de comunicações sem a apresentação de um *warrant* emanado por um juiz americano.

Uma saída para remediar esta situação é reformular o atual modelo de cooperação judiciária internacional em matéria penal e repensar os fatores definidores de jurisdição sobre dados digitais como elementos de prova, atendendo às necessidades de autoridades de segurança pública ao redor do mundo e respeitando direitos humanos. Enquanto isso não ocorre, ameaças de multas, prisões, bloqueios, além de inúmeros acordos "informais"[8] entre empresas e autoridades serão frequentes.

8. Um exemplo disso é o acordo entre a Polícia Federal e a empresa canadense "Research in Motion", fabricante do celular Blackberry. Segundo notícias, no âmbito da Lava Jato, mensagens do doleiro Alberto Youssef, só foram acessadas "porque [a PF] conseguiu convencer a BlackBerry a franquear acesso às conversas feitas por BBM, serviço de mensagens instantâneas dos aparelhos da marca". Ver BORBA, Julia; NERY, Natuza, "PF quer instalar vírus em telefone grampeado para copiar informações", Folha De São Paulo, 27 de abril de 2015, disponível em: goo.gl/NFu2Kr Acesso em 03.02.2017. Esse "canal direto" "dribla" acordos internacionais de cooperação mútua, já que sequer passam pelo Ministério da Justiça. Ver mais sobre a controvérsia em CANÁRIO, Pedro, "Relação direta entre PF e empresa canadense alarma advogados da 'lava jato'", Consultor Jurídico, 10 de novembro de 2015, disponível em: goo.gl/5vedff Acesso em: 03.02.2017.

08.

DESAFIOS DA COLETA DE EVIDÊNCIAS DIGITAIS E A COOPERAÇÃO JURÍDICA INTERNACIONAL PARA ACESSO A DADOS: VISÃO PRÁTICA

Carolina Yumi de Souza

Transcrição de Marina Arvigo.

Vou tentar tratar da cooperação jurídica internacional sobre a visão brasileira de uma maneira prática, porque trabalhei durante muito tempo na Autoridade Central Brasileira de Coordenação Jurídica Internacional.

Primeiro ponto, sem ser muito doutrinária, é que a Cooperação Jurídica Internacional é um instrumento de ajuda entre Estados soberanos para realização das finalidades do processo: seja intimar alguém, obter uma prova, ou até mesmo um bloqueio no exterior. Ela acontece, portanto, quando dentro do processo penal para sua consecução você tem um "elemento de estraneidade". O que significa isso? Eu tenho um elemento que a minha jurisdição não pode cumprir; ele está sob a jurisdição de outro país, então eu preciso do auxílio de outro país.

E a gente chega à discussão que foi trazida aqui[1]: quando você tem a parte física, é muito mais simples. Você sabe em poder de quem estão aquelas informações e como você pode fazer aquilo. Mas essa discussão não é completamente estranha ao direito internacional e à cooperação jurídica internacional. Por exemplo, ela teve muito lugar quando se tratou de quebra de sigilo bancário. Você tinha a subsidiária no Brasil ou em outros países e as sedes em outros lugares, e você via "ué, mas eu não posso intimar o Citibank daqui para me dar informações, ainda que tenha acontecido fora, dentro do próprio Citibank?". Então essa é uma discussão que volta de tempos em tempos a depender do que se pretende produzir.

Minha primeira ponderação, então, não tem necessariamente a ver com cooperação jurídica internacional, mas com um dos elementos da cooperação, que é a própria definição de jurisdição. Quando um Estado pode ou não ter jurisdição

1. Ver capítulo anterior e também ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. *Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais*. São Paulo: InternetLab, 2017, pp. 41-45. Disponível em: goo.gl/TQ7U8E

com relação a determinado dado? Qual é a lei que vai determinar isso? É muito mais um conflito de direito internacional privado do que um conflito de cooperação jurídica internacional. Então o caso do Google, por exemplo, que me parece até diferente do WhatsApp e até da própria Yahoo,[2] a solução que o TRF da 2ª Região encontrou, por exemplo, foi da nossa aplicação do direito empresarial, do direito civil com relação às próprias subsidiárias e que me parece que seria uma solução que ele aplicaria a qualquer outro caso, não necessariamente relacionado a informações digitais.

2. Os casos a que Carolina Yumi faz referência aqui são discutidos em ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. *Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais*. São Paulo: InternetLab, 2017, pp. 41-45. Disponível em: goo.gl/TQ7U8E

A grande questão que se coloca aqui é: como se define a jurisdição nesses casos? O que é um passo prévio, até. Se o Brasil decidir que tem jurisdição, e outro país entender que o Brasil não tem, você se coloca num conflito entre Estados. E mais, uma premissa para a própria implementação da cooperação jurídica internacional. Então esse é o primeiro ponto que está sendo discutido pesadamente no Brasil.

No caso da Yahoo, por exemplo, a própria saída também foi um pouco pelo direito empresarial que se entendia que a Yahoo, mais do que uma subsidiária, era uma empresa própria e que, portanto, tinha uma personalidade jurídica diferente da Yahoo internacional. Isso é diferente do caso do Google e do caso do WhatsApp. É mais complexo ainda porque é uma outra empresa [Facebook Inc.] que tem uma subsidiária aqui [Facebook Serviços Online Ltda.] e que, na verdade, também não tem nada a ver com o WhatsApp.

Então são questões muito relacionadas, pelo menos a meu ver, com a própria definição de jurisdição. Mais até do que com a cooperação jurídica internacional e, por isso, eu acho que é um passo de definição prévia.

A cooperação jurídica internacional no Brasil enfrenta uma série de dificuldades na prática. O que a gente tem é mais uma série de balizas de implementação e parâmetros do que propriamente receitas dadas.

A primeira dificuldade que é que não há no Brasil uma lei de cooperação jurídica internacional. A gente aplica aqui muito da jurisprudência, do que a própria doutrina foi construindo, da experiência internacional e obviamente dos textos tratados internacionais. A gente teve recentemente a regulação sobre a cooperação jurídica internacional no Código de Processo Civil. Então a cooperação em matéria civil tem uma regulamentação interna, nacional. Mas o que a gente vê da regulamentação em matéria penal é só o que a gente tem dentro do Código de Processo Penal, que fala somente de rogatória. Não fala do auxílio direto, que é um instrumento direto que tem sido muito mais utilizado do que a própria rogatória. A única norma interna que traz a diferenciação entre a rogatória e o auxílio direto é o Regimento Interno do Superior Tribunal de Justiça (STJ). Tudo começou com a Resolução nº 9, e essas normas foram incorporadas pelo Regimento Interno. Tem uma distinção que, para quem não tem em seu país parece não fazer sentido, e para gente é muito complicado porque o STJ tem aplicado de forma até aleatória é a distinção entre auxílio direto e a rogatória. Pela regulamentação interna, se há necessidade de juízo de delibação, seria rogatória. Se não há necessidade de juízo de delibação, seria o auxílio direto.

Com relação aos próprios instrumentos de cooperação, como foi colocada uma informação do relatório[3], de fato eles não foram pensados, principalmente os tratados, para uma cooperação um pouco mais célere. Isso é um problema que a gente tem visto em vários outros tipos de cooperação

3. Referência a ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. *Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais*. São Paulo: InternetLab, 2017, pp. 41-45. Disponível em: goo.gl/TQ7U8E

jurídica internacional. Essa dicotomia, ou essa briga, entre cooperação formal versus cooperação informal na verdade também é uma discussão bastante antiga em vários outros âmbitos e que merece discussão em vários outros foros internacionais. A OEA e a ONU discutem muito isso. Foram criados mecanismos paralelos, e até foros paralelos, relacionados a informações, a coleta de evidência em meio digital.

Eu acho que a gente pode citar a própria rede criada no âmbito da Interpol de coleta e troca de informações e o 24 por 7, que foi criado pelo G8 no próprio âmbito da OEA. Mas, do meu ponto de vista, pelo menos para cooperação jurídica internacional, isso também nos últimos tempos tem tido uma conciliação. E como isso tem se mostrado em torno dos instrumentos? A cooperação jurídica internacional é fundamental, do ponto de vista informal, para você obter as informações preliminares para embasar o seu pedido formal e também para preservação dos dados. Mais do que para a obtenção dos dados por meio da cooperação jurídica internacional informal. A cooperação informal é fundamental para a preservação desses dados. Por quê? Justamente porque é tudo mais célere, o tempo de guarda desses dados é muito menor. Você guarda esses dados de maneira informal antes e depois você faz o pedido de cooperação jurídica internacional formal.

Eu acho que o pedido de cooperação de maneira formal nunca vai acabar sendo substituído, por isso na verdade ele tem que ser complementado. Até porque ele envolve a atividade de jurisdição de muitos outros Estados e muitas das vezes há necessidade de você ter o pronunciamento formal do Poder Judiciário ou das autoridades administrativas daquele determinado Estado. Então com relação também à cooperação jurídica internacional informal versus cooperação jurídica formal, eu acho que elas devem coexistir, especialmente na busca desse tipo de evidência. Obviamente o MLAT tem que ter uma for-

ma mais célere de acontecer, de se comunicar. Mas, na prática, a gente tem um cumprimento de um pedido de cooperação jurídica internacional com os Estados Unidos, por exemplo, se todas as informações estiverem corretas, em 3 meses você tem o retorno. Para a parte de evidência digital, de fato pode parecer pouco tempo, por isso nós precisamos de preservação, mas hoje os mecanismos de cooperação jurídica internacional são muito mais céleres. Claro que eu disse e trouxe aqui o exemplo dos Estados Unidos, claro que vai depender muito de que país e com que tipo de dado você está lidando. E por quê isso?

Uma das características da cooperação jurídica internacional e que na verdade é muito importante e é fundamental a ela e que isso causa muito stress, digamos assim, às autoridades que têm que trabalhar com ela é a questão da lei aplicável na cooperação jurídica internacional. Qual é a lei aplicável à cooperação? É a lei aplicável do país em que a medida for produzida. É aquela lei que vai reger como aquela prova vai ser produzida, mesmo que ela seja diferente do próprio país que tem a jurisdição para aquele processo. Mas ainda assim isso é complexo porque você tem que entender um outro ordenamento jurídico, mas não é só entender um outro ordenamento jurídico. Na verdade, o que você tem na cooperação é uma interação dos sistemas jurídicos. Você tem a lei aplicável do país que tem a jurisdição e você tem a lei aplicável do país em que a medida vai ser feita. E na verdade quando essa prova volta, você tem que ver como as duas leis se compatibilizam para você introduzir de forma válida no processo.

Essa questão da lei aplicável vai reger, no país que tem a jurisdição, o pedido de cooperação internacional. Então a questão, por exemplo, da extração de dados extraídos de um aparelho que foi apreendido, um aparelho celular, por exemplo. No Brasil a jurisprudência acaba entendendo, o próprio Supremo Tribunal Federal, que na verdade se você tem a obtenção de

um determinado aparelho, você obviamente tem acesso aos dados, você pode ter acesso a tudo que está lá dentro. Nos Estados Unidos, por exemplo, a discussão é um pouco diferente. Você tem que ter uma ordem específica com relação aos dados e também conseguir demonstrar que você quer aqueles dados que estão dentro daquele aparelho. E tem alguma discussão inclusive da busca e apreensão de computadores.

Então o pedido que saia do Brasil, por exemplo, não pode limitar na sua descrição que ele quer ter acesso a um dado em um determinado aparelho e acreditar que esse pedido embasaria o acesso aos dados que estão dentro desse aparelho e que poderia usá-los livremente por meio de um pedido de cooperação jurídica internacional. O pedido que tivesse que ser feito para os Estados Unidos, tem que especificar exatamente qual o objeto que está sendo pedido pra lá, exatamente qual a finalidade do que está sendo pedido na produção desses dados. Então por mais que a nossa lei permitisse isso, a gente tem que adaptar o nosso pedido e até mesmo a nossa autorização judicial para conseguir a obtenção judicial nesse país. Talvez um outro país tenha alguma regra diferente com relação a isso, mas na verdade essa é a regra que a gente tem que buscar e ver como compatibilizar o pedido de cooperação jurídica internacional.

De fato, esse é o papel que tem sido exercido, e por isso a gente acaba conhecendo um pouco o que acontece pela própria autoridade central, que no Brasil é o Ministério da Justiça, para entrar em contato com as outras autoridades dos outros países para averiguar quais são os requisitos para elaboração desses pedidos. Por exemplo, nos Estados Unidos, a gente se comunica muito com a autoridade central de lá por meio de e-mail, conversas telefônicas, e várias das respostas negativas que a gente tinha com relação a evidências por meio de troca são encaminhadas até de maneira mais informal por meio de e-mail, etc., de maneira que a gente acaba nem mandando

pedido de cooperação jurídica internacional para lá que de antemão a gente já sabe quais seriam as dificuldades e os óbices que aquele país apresentaria.

Com relação aos pedidos exatamente de cooperação jurídica internacional em termos de números, a gente vai ver que as dificuldades para cumprimento desses pedidos são muito próximas uns dos outros. Até porque o Brasil tem uma pequena experiência em termos de cooperação jurídica internacional para obtenção desses dados. Os dados que me foram encaminhados pela autoridade central, uma série histórica, a gente vê que cerca de 115 pedidos de cooperação jurídica internacional foram feitos na nossa história envolvendo obtenção de dados, obtenção de evidências por meio digital.

Para se ter uma ideia do que isso representa, eu estou aqui com os dados referentes aos anos passados. Até abril desse ano [2017], só de cooperação jurídica internacional em matéria penal, nós já temos 737 pedidos. Em matéria civil, 954. O ano passado foram 1912 pedidos de cooperação jurídica internacional em matéria penal e 3298 pedidos em matéria civil. E essa série se repete mais ou menos nesses números, e a gente vê que, então, nessa questão de obtenção de evidências por meio digital os números são absolutamente muito menores.

Entrando no mérito desses pedidos, quanto à espécie de pedido que já foi feita com relação à obtenção dessas evidências digitais, temos: login de acesso, dado cadastral do e-mail em rede social, número de IP do computador, quebra do sigilo de conteúdo do e-mail em chat, Twitter, redes sociais, e interceptação em tempo real, o que se costuma chamar de grampo telemático.

Por que a gente não tem conseguido o cumprimento de muitos desses pedidos? As causas são muito próximas à falta de cumprimento em outros pedidos de cooperação jurídica internacional, e algumas específicas. Eu separei o exemplo dos

/ QUANDO UM ESTADO PODE OU NÃO TER JURISDIÇÃO COM RELAÇÃO A DETERMINADO DADO? /

/ OS INSTRUMENTOS [CLÁSSICOS] DE COOPERAÇÃO NÃO FORAM PENSADOS PARA UMA COOPERAÇÃO MAIS CÉLERE. /

Estados Unidos, que na verdade congrega 90% dos nossos pedidos de cooperação jurídica internacional dessa matéria.

Uma das primeiras causas de recusa dos pedidos de cooperação jurídica internacional dos Estados Unidos, e que é muito comum nos outros pedidos de cooperação jurídica internacional, é a ausência de "probable cause". Trazendo um pouco para o que a gente tem, de nexo causal. A forma como o caso é construído aqui no Brasil é diferente da forma como o caso é construído nos Estados Unidos. E muitas das nossas autoridades não estão acostumadas a essa forma de construção de caso e, por isso, isso é um problema. Pelos números, vocês viram, a gente não está falando aqui do Ministério Público Federal ou um dos grandes casos da Lava Jato, etc. A gente tem quase 2 mil pedidos em um ano que advém das mais diferentes autoridades do país – de lugares que algumas autoridades nunca fizeram um pedido de cooperação jurídica internacional.

Como isso acontece? A forma de construção do caso aqui é: "Essa pessoa fez aquilo. Ela tem um e-mail no exterior e eu quero aquele e-mail para ver como aquele e-mail pode me ajudar no caso". Isso não funciona, principalmente nos Estados Unidos. Você tem que demonstrar por quê você acha que aquela pessoa fez aquilo, qual é a ligação daquele e-mail com aquilo que você está querendo, quer dizer, qual o link daquele e-mail com o caso e qual a finalidade do que você precisa, o que você pretende demonstrar com aquele e-mail, por exemplo.

Essa é uma das causas de recusa que é comum a diversos pedidos de cooperação e não poderia deixar de ser comum na recusa a pedidos de evidências digitais. Principalmente nesses casos específicos em que você tenta utilizar e achar dentro dessas conversas ou desses dados, qualquer tipo de pista, digamos assim, que possa te ajudar a ir para o próximo passo. Ou seja, você não vai numa investigação, na maior parte dos casos, sabendo o que aquilo pode te demonstrar. Na verdade,

você tenta partir daqueles dados, usando como ponto de partida para a sua investigação. Então essa é uma primeira causa de recusa que é comum aos outros casos, como eu disse, e que não podia deixar diferente para os pedidos de cooperação jurídica internacional.

O segundo caso que é comum é para outras hipóteses, mas mais para os casos de evidência digital, na verdade mais para os casos de bloqueio ou retirada do ar ou qualquer página da internet, nos Estados Unidos é relacionada à Primeira Emenda à Constituição que, para eles, é bastante ampla. Protegendo a liberdade de expressão, enfim, a liberdade de imprensa. Então algumas ordens emanadas de juízes daqui, para que sejam retirados do ar sites com conteúdo racista, com, enfim, ou até conteúdo discriminatório de outras formas, não são atendidas pelos Estados Unidos porque eles entendem que o conteúdo daqueles sites na verdade está protegido pela Primeira Emenda.

E a terceira causa de recusa com relação aos pedidos envolvendo evidências telemáticas na verdade é bem específica com relação às interceptações em tempo real ("grampos telemáticos"). Os Estados Unidos respondem a esse tipo de pedido, na verdade, de que é impossível o cumprimento desses pedidos em virtude de requerimento de autoridade estrangeira.

Alguns motivos para isso, segundo algumas respostas que a gente tem obtido, seriam que na verdade a lei estadunidense não permite esse tipo de pedido de autoridades estrangeiras e que na verdade esse tipo de medida só pode ser determinada por um juiz estadunidense para determinados tipos de crimes. Então ela seria uma medida bastante restrita e que não alcançaria o atendimento dos pedidos para autoridades internacionais. Essa é a resposta que a gente tem obtido, então essa é a outra peculiaridade do pedido de obtenção de evidências de maneira digital nos Estados Unidos. Que, como

eu disse, tem cerca de 90% dos nossos pedidos de cooperação jurídica internacional.

No caso dos pedidos do WhatsApp, eles entram em uma outra categoria muito específica e também, com relação ao não cumprimento dos pedidos que já foram mandados para lá, a resposta do governo norte-americano na verdade tem sido: a impossibilidade de cumprimento vem da própria regulamentação e da própria forma de trabalho do WhatsApp. Dizem que eles não guardam esse tipo de dado e que, portanto, eles não podem cumprir esse tipo de pedido porque simplesmente a empresa não possui [dados] com relação às mensagens que foram enviadas. E com relação às mensagens que não foram enviadas, a empresa só guardaria esse tipo de informação por 30 dias. Então também quando chegam os pedidos de cooperação jurídica internacional, já não haveria como obter essas informações porque elas já não estão mais disponíveis.

Essas são as causas que a gente tem, no geral, do não cumprimento da cooperação jurídica internacional. Mas, como eu disse, a nossa experiência na parte de cooperação jurídica internacional brasileira por meio da obtenção de evidências é bastante pequena. Para se ter ideia, entre 115 ou 120 pedidos que eu mencionei, alguns ainda estão em andamento mas a gente obteve, de fato, 15 pedidos de cooperação jurídica internacional desses que a gente encaminhou. Então a experiência é pouca, a experiência é da própria discussão das autoridades internas, que é feita em foros internacionais voltados para isso.

O Brasil, em termos de postura internacional, debate muito esse assunto, mas de fato a gente não está inserido formalmente em nenhum âmbito dessas discussões. A própria ONU agora tem discutido muito a elaboração de uma Convenção de Cibercrime que teria os meios de cooperação jurídica internacional voltados exclusivamente para isso. Vocês sabem que a gente não acedeu, não aderiu à Convenção de Budapeste

por questões de política internacional também. Essa posição tem sido revista pelo Itamaraty (Ministério das Relações Exteriores) porque era uma questão mesmo meramente de política internacional. Eles diziam que o Brasil não acedia a Convenções internacionais das quais não tivesse participado das negociações. Em tese, esse seria o grande motivo para não ter aderido a Budapeste. Mas esse posicionamento tem sido revisto, não tem nenhum sentido a gente ficar de fora de algumas Convenções. Eu acho que isso depende muito da matéria. Mas de fato como base da cooperação jurídica internacional, inclusive para esses pedidos, o que a gente usa são os acordos bilaterais com os países que a gente tem, que podem não ter sido previstos especificamente para esses casos mas que são utilizados e que contém medidas que podem ser utilizadas para obtenção desse tipo de evidência. E também algumas Convenções multilaterais com alguns meios mais ágeis, em especial as Convenções da ONU e até aquela da OEA.

Esse é o retrato da cooperação jurídica internacional do Brasil com relação a esses dados. O que eu acho, para finalizar, é que a gente deve, na verdade, progredir nessa participação de foros internacionais. As discussões com esse tipo de medida têm sido bastante avançadas. Dentro mesmo de Budapeste, o Conselho da Europa tem milhares de manuais, regulamentações, recomendações para que os países sigam nessa matéria. Eu não sei se de fato elas são efetivas, mas eu sei que o material produzido é bastante vasto e os encontros que eles têm feito também. Essa questão da cooperação informal vai ter que aumentar também bastante, mas sempre de maneira paralela à cooperação formal para obtenção, ao final, desses dados.

PERGUNTAS/RESPOSTAS

< PERGUNTA > No cerne das respostas que a autoridade americana, que os Estados Unidos acabam dando ao Brasil,

é exatamente onde estariam as proteções em questões acessórias no direito. Será que o que eles estão protegendo lá não seria o que a gente deveria primar por proteger aqui também?
< PERGUNTA > Sobre a cooperação jurídica informal: o que seria? Temos exemplos disso? Em especial na coleta de evidências em meio digital. A gente vê casos inclusive ligados à própria Operação Lava Jato, de conversas de autoridades brasileiras com empresas no exterior e acho que valeria à pena esclarecer um pouco.
< CAROLINA > Como eu coloquei, no caso da cooperação jurídica internacional, as discussões se dão mais do ponto de vista formal até do que propriamente material. A gente acaba não entrando muito na discussão do que está sendo privilegiado no outro ordenamento em termos da discussão da privacidade. E até do ponto de vista processual, que é mais a minha área, na verdade o que eu acho que se coloca lá é mais uma questão de obediência às regras postas para cumprimento de pedidos de cooperação jurídica internacional. A discussão da privacidade lá, para as, enfim, com relação a essas questões do WhatsApp ou até do Facebook, é muito importante, porque ela tem reflexo sobre aquilo que a gente vai conseguir. E talvez ela vá influenciar o que a gente vá decidir aqui ou não. Mas do ponto de vista da cooperação jurídica internacional, é mais sob o prisma de não alcançar os standards que estão lá postos. A gente não entra na discussão sobre a validade ou a própria eficiência desses standards. A discussão da privacidade em si é muito mais complexa nesse ponto, quando se coloca jurisdição penal versus privacidade. Então é uma discussão que deve estar no mundo todo.

Com relação aos mecanismos de cooperação jurídica internacional, eu acho que dá para juntar um pouco as duas coisas. Na verdade, quando se utiliza o MLAT, também os requisitos vão depender de cada país. Há países que são mais

formalistas, há países que são menos, mas por exemplo. No auxílio direto, se você tem um Tratado, você não precisa mais de uma tradução juramentada para nenhum país. Somente para alguns muito específicos, quando você está falando de rogatória. Nos Estados Unidos, por exemplo, que é o nosso exemplo, é uma simples tradução e na verdade é comunicação direta por e-mail, por WhatsApp, por telefone. A grande questão então é: todo o procedimento pode ser agilizado, mas quando você tem de fato a produção de uma jurisdição para outra, para ser colocada no processo, aí essa parte final não me parece muito como possa ser agilizada. Porque ela depende de uma análise de legalidade e de validade do que foi produzido no outro país. Afinal, é um país se comprometendo com o outro de que o que ele está dando foi produzido legalmente no seu próprio país. Então essa parte final de chancela de produção de acordo com as normas, eu não sei se tem muito como ser flexibilizado. Mas com relação ao contato com as outras autoridades, é fato que tem sido bastante ágil, principalmente da parte do Ministério Público Federal e de alguns juízes.

A gente tem um problema bem mais sério na cooperação jurídica internacional, quando a gente está falando dos pedidos da defesa, o que não tem a ver com burocracia de procedimentos. Inclusive nos Estados Unidos, que é o nosso caso, a manifestação é que não se atende por MLAT, alguns casos foram flexibilizados, mas em geral não se atende por MLAT pedidos oriundos da defesa. Então a gente entra em outra discussão, inclusive de paridade de armas. É processo, mas também essa é outra discussão. Então não é uma questão do instrumento, do mecanismo.

Alguns pedidos ainda hoje acabam sendo atendidos ou não, mas a postura definitiva dos Estados Unidos com relação a isso é que se de fato for importante para o processo como

um todo, sim. Mas se foi deferido pelo juiz e na verdade é uma prova da defesa, não. Não deixa de ser uma prova da defesa, não importa quem tenha deferido. Pelo sistema deles, essa questão de prova das partes é muito clara: quem está deferindo o que? Então não importa a autoridade que está mandando, o que importa é a própria natureza e a finalidade da prova.

< PERGUNTA > (áudio não capturado)

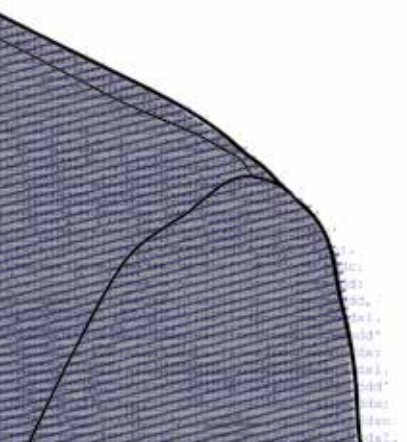
< CAROLINA > Com relação ao WhatsApp e etc., na verdade eu acho que a gente vai até que ver como vai ficar a situação aqui já que os pedidos têm sido relacionados para as empresas aqui mesmo. Então a questão da cooperação, se for definida a nossa jurisdição para isso, deixou de ter um pouco de relevância. Mas esse seu caso não é um caso de burocracia do sistema, é um caso mais de provas produzidas por ordem da defesa. Então é uma outra questão.

E só por fim, com relação à cooperação jurídica internacional, a gente tem cooperação jurídica internacional numa definição clássica que são os meios clássicos de cooperação jurídica internacional e as redes informais de cooperação jurídica internacional, que são aquelas redes formadas por todas as autoridades, além do contato direto que tem cada uma. Mas o que eu mencionei aqui mesmo foram essas redes institucionais de troca de informações. Você tem informações que podem ser trocadas entre as autoridades, até para ajudar nas investigações que estão acontecendo, informações prévias. E que seriam até administrativas e que auxiliam na própria troca de informações. Então, por exemplo, uma cooperação informal mas que é absolutamente formalizada, digamos assim, as informações foram trocadas entre unidades de inteligência financeira. Por exemplo, entre o COAF. Ela não é formalizada como uma cooperação formal, ela não se destina a um processo ou a uma investigação propriamente dita, mas ela é uma rede de cooperação informal. É isso.

09.

REFORMA DO SISTEMA MLAT ENTRE PRIVACIDADE E EFICIÊNCIA: OS DILEMAS DO ACESSO TRANSNACIONAL A DADOS DE USUÁRIOS

Greg Nojeim



Tradução de Ana Luiza Araujo. Revisão técnica de Jacqueline de Souza Abreu.

Meu nome é Greg Nojeim. Eu trabalho para o Centro para Democracia e Tecnologia. Eu quero agradecer ao InternetLab por fazer possível a minha vinda até aqui. Dennys, Francisco, Mariana, Jacqueline toda a equipe, realmente muito obrigado. Eu realmente agradeço pela oportunidade. Eu não tenho muitas oportunidades para falar com estudantes de direito, mas isso sempre me energiza porque os alunos tendem a ter perguntas muito boas e eu acho isso muito divertido. Eu vejo que muitas pessoas não estão usando fones de ouvido, é realmente o caso que tantas pessoas entendem inglês? Como é que nós nunca vemos vocês nas ruas quando estamos pedindo informações? Bem, apenas mais um obrigado e esse é o agradecimento por terem vindo, vocês estão em uma cidade maravilhosa, há um milhão de coisas para fazer aqui. Obrigado.

Bom, com isso dito, deixem-me contar um pouco sobre a minha organização. Eu trabalho para um grupo de direitos humanos, o Centro para Democracia e Tecnologia. Nós estamos sediados em Washington DC, temos cerca de 25 pessoas, metade de nós somos advogados. Adivinhem? Nós contratamos estagiários, mas nós não os pagamos. Se você é capaz de vir a Washington, se você estiver interessado em estagiar, venha aqui depois e nós podemos falar sobre isso. Sim, a Riana foi estagiária no CDT dez anos atrás e olhem onde ela está!

Bem, a minha peça do quebra-cabeça no Centro para Democracia e Tecnologia é tentar garantir a privacidade contra a invasão pelo governo ou por outros governos também – não apenas o governo dos EUA. Nossa maior iniciativa nos Estados Unidos é fazer com que a lei dos Estados Unidos, o estatuto[1], esteja de acordo com o que os tribunais têm decidido até agora, que é que quando as autoridades de investigação querem ter acesso ao conteúdo de comunicações [eletrônicas], elas precisam

1. [Nota da editora] A referência aqui é provavelmente ao Stored Communications Act (18 U.S.C. §§ 2701-2712), estatuto de 1986, disponível em: goo.gl/oDH07u

obter uma ordem judicial, um mandado [*warrant*] baseado em uma constatação de causa provável [*probable cause*]. Essa é uma das nossas principais iniciativas; nós ganhamos essa questão nos tribunais até agora, mas nós ainda não temos isso escrito na lei.

Eu gostaria de dizer que a especialidade da minha organização é reunir pessoas de diferentes origens dentro de nosso espaço, não se trata de origens étnicas ou qualquer assim, é sobre os interesses de autoridades de investigação, os interesses das empresas e os interesses dos consumidores e os interesses dos acadêmicos. Trazê-los todos ao redor de uma grande mesa e discutir questões muito difíceis e nós temos tem um monte de questões difíceis hoje em dia com a nova tecnologia.

Neste caso, o difícil problema que eu quero colocar na frente de vocês é: ajudar as autoridades de investigação, incluindo autoridades no Brasil a ter acesso ao conteúdo de comunicações, incluindo conteúdos guardados por empresas estadunidenses e ao mesmo tempo proteger os direitos dos brasileiros e estadunidenses e de outras pessoas em todo o mundo, porque os provedores que guardam esses dados têm uma base de usuários do mundo todo. Eu não vou falar sobre a vigilância que Edward Snowden divulgou. Eu não vou fazer isso, a não ser que vocês me perguntem sobre isso. O motivo pelo qual eu não vou fazer isso é porque esse é um tipo diferente de vigilância, ela está sob um regime legal totalmente diferente nos Estados Unidos. Na verdade, não há um bom regime legal para essa vigilância, ela é muito permissiva particularmente no que diz respeito às pessoas fora dos Estados Unidos, se vocês me perguntarem sobre isso – e espero que o façam – existem alguns grandes desenvolvimentos sobre os quais eu poderia falar com vocês.

Em vez disso, eu quero falar é sobre a vigilância por razões criminais. A vigilância de Snowden era sobre segurança

nacional. Vou falar da vigilância usada para resolver e prevenir crimes. E a necessidade de realizar essa vigilância que as autoridades de investigação têm está crescendo o tempo todo. E há obstáculos para isso, Riana falou sobre um: um é a criptografia de comunicações. Eu vou falar sobre outro: geografia. Lidar com o fato de que a polícia muitas vezes precisa de acesso a dados que estão fora do seu país e certamente distantes da cena do crime que estão investigando.

Isso não é novidade para vocês, mas era novidade para mim. Houve uma revolução tecnológica, nós movemos dados de nossas gavetas, de nossas casas, para computadores e, em seguida, até mesmo fora dos computadores, na nuvem. Agora, os dados de que os agentes necessitam estão na mão de terceiros, estão guardados por empresas como Google, Microsoft, Facebook, Twitter e nem todos eles os têm da mesma maneira e então isso cria alguns desafios para as autoridades de investigação. A Microsoft é o que eu chamo de "localizadora de dados", pois quando você se inscreve para uma conta do Hotmail a Microsoft te pergunta "onde vocês está?" e eles estão te perguntando isso porque eles vão localizar os seus dados perto de você, muitas vezes em seu próprio país.

Quanto ao Google, eu não acho que eles pedem isso. Eles não me pediram isso quando eu configurei a minha conta do Gmail. Mas o Google é diferente, o Google movimenta seus dados. O Google é o que eu chamo de "balanceador de carga", eles movem os dados pela sua rede para equilibrar a carga. Se as coisas estão ocupadas na Índia, eles podem mover os dados dali para outro lugar onde está menos ocupado para que eles possam equilibrar a carga em sua rede. O Google também quebra os dados, ele os divide em diferentes pedaços para que então mesmo um email possa ser guardado em pacotes que estão em lugares diferentes, até diferentes países.

Assim, enquanto a Microsoft está tentando colocar os dados em uma base estática e pode viver com uma regra que fala sobre a localização dos dados como base para a jurisdição, para empresas como o Google, que movem os dados por aí, não é uma boa norma essa ideia de ter a localização como determinante da jurisdição. E para nós indivíduos, uma coisa que nós realmente gostaríamos de saber é onde estão nossos dados, o que pode ser algo que não é respondível por uma empresa que está movendo dados como o Google. Mas nós também queremos saber qual lei está sendo aplicada aos dados e nós não podemos ter certeza disso, a não ser na medida em que a empresa nos diz que lei eles pensam que se aplica aos dados.

Para as autoridades de investigação é ainda mais difícil. Você tem um policial aqui em São Paulo, ele está tentando investigar um crime, ele quer acesso a dados que podem estar guardados em Seattle, Washington, podem estar guardados no Silicon Valley, que podem estar em outro lugar, podem estar na Irlanda. Mas ele precisa do acesso a esses dados para resolver o crime e às vezes ele precisa de acesso aos dados de pessoas que não são brasileiros porque os crimes que mesmo a polícia local está investigando hoje em dia podem ser cometidos por pessoas que estão fora do país, não nos Estados Unidos, seja na França, eles podem estar na China, eles podem estar em qualquer lugar. Nós temos que lidar com este problema, os criminosos não vão esperar, eles não vão deixar de cometer seus crimes enquanto nós descobrimos como resolver este problema e nós simplesmente não podemos continuar esperando.

A LEGISLAÇÃO ATUAL

Antes de falar sobre o que eu acho que seja o espaço de solução para o problema, eu quero falar sobre quais são as regras que regem a vigilância agora. Cada país tem sua própria lei de vigilância e a realidade é essa porque, como muitos dos

grandes provedores estão nos Estados Unidos, a lei dos EUA torna-se relativamente importante nesta área. Então eu vou falar para vocês um pouco sobre o que ela exige e o que ela exige dos provedores que operaram sob ela. O *Stored Communications Act*[2] foi escrito em 1986. Foi há muito tempo. O filme mais popular na época era Top Gun, com Tom Cruise. Isso diz há quanto tempo foi isso. Eles realmente não atualizaram a lei de uma maneira substancial, aconteceram algumas mexidas ao longo do caminho, mas não houve nenhum esforço real para atualizar o estatuto desde que foi escrito há quase 30 anos. Tivemos o mesmo debate nos Estados Unidos sobre o qual o professor Sampaio Ferraz falou ontem.[3] Tivemos o mesmo debate: uma comunicação eletrônica, como um email, é como cartas enviadas pelo correio ou é como interceptar uma comunicação através de uma escuta? Tivemos exatamente o mesmo debate e os debatedores foram, provavelmente, os mesmos tipos de pessoas que estavam debatendo aqui. Tivemos autoridades de investigação, tivemos os grupos de privacidade, e tivemos as empresas, todos tentando chegar a decisões sobre quais regras se aplicariam.

2. [Nota da editora] A referência aqui é provavelmente ao Stored Communications Act (18 U.S.C. §§ 2701-2712), estatuto de 1986, disponível em: goo.gl/oDH07u

3. [Nota da editora] Ver texto de Tércio Sampaio Ferraz Junior nesse livro ou em vídeo goo.gl/Mkvzrx

Nos EUA nós chegamos a um compromisso, nós sempre acabamos com algum acordo [*compromise*]. Mas nós tivemos um compromisso e o compromisso era este: para o conteúdo que provavelmente não está abandonado, que é algo que a pessoa provavelmente vai querer usar no futuro, adotamos uma regra que diz que é preciso haver uma ordem judicial que é chamada de mandado [*warrant*] baseado em uma descoberta de causa provável, que é um nível de prova muito alto. Ela exige a demonstração de uma probabilidade de crime e uma probabilidade de que a informação solicitada irá ajudar

a resolver esse crime. Ambas as formas são necessárias para obter conteúdo nos Estados Unidos. Para não-conteúdo ou informações relativas a quem você enviou um email e quem enviou um email para você, é um nível mais baixo – também há uma ordem judicial, mas você não precisa ter aquele mesmo nível de conexão com o crime e aquele mesmo nível de certeza sobre o cometimento de um crime. Para as informações que nós chamamos de informações do assinante [*subscriber information*], é um nível ainda mais baixo. Essas são informações como quem teve esse endereço de IP – Internet Protocol Address – nesse dia, nessa hora e isso é relevante para uma investigação criminal porque isso mostra onde você foi na Internet, quem está na página naquela hora. Informações como a quem pertence um endereço de email, não é necessária uma ordem judicial sob a lei dos EUA. Apenas uma intimação [*subpoena*], que é uma demanda escrita por autoridades de investigação. Uma intimação é o suficiente.

Você pode dizer que o resultado faz algum sentido: para os dados mais sensíveis, você precisa de mais provas de crimes e você precisa da autorização de um juiz; para dados sensíveis de nível intermediário – informações de tráfego – você precisa da autorização de um juiz, mas você não precisa do mesmo nível de prova; para as informações menos sensíveis, você não precisa da autorização de um juiz e você não precisa de um alto nível de prova.

Eu acho que isso saiu próximo do correto e é muito semelhante às regras que foram adotadas no Brasil[4] e é semelhante às regras adotadas em outros países. E mais uma coisa, aquela regra sobre a necessidade de uma causa provável, ela se aplica sem discriminação. Se você está nos Estados Unidos e autoridades investigativas estadunidenses querem

4. [Nota da editora] Ver, por exemplo, ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. Disponível em: goo.gl/TQ7U8E

investigar você ou eles querem me investigar, é a mesma regra para nós dois. Não é discriminatório.

O SISTEMA MLAT

Então avance o relógio de 1986, quando não havia o Google, não havia Twitter, não havia Facebook, para hoje. Quando todas essas companhias que possuem todos esses dados existem e elas têm uma base de dados global. O que os Estados Unidos fizeram? Eles pegaram a lei que havia sido escrita ao redor de uma regra doméstica e a aplicaram para os pedidos internacionais que eles estavam recebendo – e outros países fazem a mesma coisa. Quando um país quer acesso a uma busca física conduzida em outro país, eles acham que há uma evidência em uma casa na França e eles querem que uma busca seja feita nesta casa na França, eles não enviam os seus agentes de segurança pública pela fronteira na França para fazer a busca na casa. Eles vão às autoridades francesas com as quais eles têm um *acordo de cooperação judiciária mútua [Mutual Legal Assistance Treaty* – MLAT] e pedem aos franceses que realizem a busca naquela casa na França e era assim que os estadunidenses faziam com dados. Eles os tratavam como buscas físicas, não havia outro regime para dar assistência.

Então quando outro governo quer dados guardados de um provedor estadunidense, o governo estadunidense diz a esse governo "não peça ao provedor, peça para nós e nós iremos solicitar por você um mandado sob a lei estadunidense para conseguir essa informação"; é dessa maneira que tem funcionado por muitos anos, até eu acho, bem recentemente.

Com o que se parece esse processo? Eu sou o policial em São Paulo, eu quero dados que estão sob a guarda de uma empresa estadunidense, eu vou à autoridade central no Brasil, que foi representada aqui ontem pela Carolina Yumi de

Souza[5], e digo "nos ajude a conseguir esses dados". O que ela faz? Ela não vai ao Google e diz "nos dê os dados" – ela pode, mas ela não deve. Ela vai ao Departamento de Justiça dos Estados Unidos – a nossa autoridade central – e ela diz "nós queremos esses dados" e o Departamento de Justiça diz "bem, se você quer esses dados, nos dê o que nós precisamos para ir até um juiz estadunidense e sustentar a causa provável". Isso é o que acontece na maioria das demandas para entrega de conteúdo que fracassam – fracassam por causa de uma falha em entregar informações suficientes para atingir esse grau de causa provável.

5. [Nota da editora] Ver apresentação em goo.gl/4Mh81g

Nos Estados Unidos é ilegal para um provedor estadunidense revelar conteúdos sob a jurisdição estadunidense para qualquer um sem um mandado emitido por um juiz estadunidense baseado em uma constatação de causa provável. Agora, já me disseram que alguns dos provedores entregam conteúdos às autoridades brasileiras quando elas os requisitam.[6] Como isso pode acontecer? Eu acho que isso acontece ou porque eles estão assumindo a posição de que os dados guardados não estão sob a jurisdição estadunidense. Se eles são uma Microsoft, eles têm dados localizados no Brasil, a Microsoft assumirá a posição de que o processo brasileiro irá engloba-la. Se eles forem uma companhia que move dados como um Google, eles provavelmente estão assumindo a posição de que há um conflito de leis e sob o conceito da lei internacional de *comity* (respeito pelas leis de diferentes países), eles fazem uma análise e se o interesse do Brasil pelos dados excede o interesse estadunidense, eles fazem a entrega dessa maneira.

6. [Nota da editora] Tal afirmação se dá com base em julgados do Superior Tribunal de Justiça que condenaram a Google Brasil e a Microsoft Informática a fornecerem dados de conteúdo de email no âmbito de investigação. Ver, por exemplo, VIEIRA, Victor. STJ manda que Google entregue dados arquivados nos EUA. *Consultor Jurídico*. 6 de junho de 2013. Disponível em: goo.gl/uhYVDn

Além desse [padrão de] causa provável incorporada na lei estadunidense, há outras proteções que estão incluídas, como para liberdade de expressão. O Departamento de Justiça dos Estados Unidos não auxilia quando um pedido para uma entrega quando ela violaria os direitos de livre expressão de uma pessoa. Eles exigem uma dupla incriminação, o que quer dizer que não há esforços do Departamento de Justiça dos EUA para auxiliar com o processo de um crime de insulto a um rei na Tailândia; [se e quando] eles recebem esses pedidos, eles os recusam. E eles apenas aceitam os pedidos para crimes graves para os quais a pena seria de um ano ou mais.

Houve um caso sobre o qual o Departamento de Justiça gosta de falar, em que eles receberam um pedido de MLAT para o caso de uma galinha roubada. E eles disseram "não, isso é uma galinha roubada, nós não vamos nos incomodar com isso porque não é o suficiente, não é importante o suficiente para colocar os recursos".

Informações suficientes são dadas ao Departamento de Justiça, eles entram com o requerimento para o mandado de um juiz, o juiz concede o mandado, a ordem vai para o provedor, o provedor faz a entrega para o Departamento de Justiça nos Estados Unidos, o Departamento de Justiça nos Estados Unidos extrai os seus dados relevantes e os entrega para a autoridade central no Brasil, a autoridade central no Brasil os repassa para o policial em São Paulo em uma média de dez meses após o seu pedido. Ele cresceu uma longa barba enquanto esperava por esses dados aparecerem para um crime na Internet que ele está investigando. Não é preciso ser um cientista para saber que esse não é um sistema que irá funcionar. Além disso, para aquele policial em São Paulo que quer esses dados, todo esse sistema está opaco para ele, ele não consegue ver através dele; ele não sabe se os dados estão vindo, ele não sabe quando eles virão e é muito frus-

trante para ele fazer isso. Eu quero dizer, no lado dos EUA é uma coisa cara, custa dinheiro para contratar o procurador que vai até o juiz – você tem que contratar o juiz também – e para reunir os dados e para fazer essas entregas. Isso leva tempo e isso leva dinheiro.

E vocês sabem o que mais? Esses procuradores que estão recebendo esses pedidos da autoridade central nos Estados Unidos, eles têm outras coisas para fazer. Há grandes crimes locais que precisam ser resolvidos e se eles não forem resolvidos, eles ameaçam a carreira do procurador. Então se ele tem 100 casos, um deles é do Brasil, 99 deles são locais, qual deles ele irá priorizar? Quais você priorizaria? É dessa maneira que isso tem funcionado. Eles apenas não colocaram os recursos e o pessoal para processar os pedidos que eles estão recebendo regularmente. Os Estados Unidos recebem mais de três mil pedidos de MLAT a cada ano e eles mesmos fazem cerca de mil pedidos de MLAT.

Quando você olha para o quadro geral aqui, o que os Estados Unidos estão essencialmente fazendo é exportar a sua própria lei, certo? Eles recebem esses pedidos, eles aplicam as normas estadunidenses para o resto dos pedidos que estão vindo do resto do mundo. Isso significa que para um país como o Brasil, no qual evidências digitais se tornam mais difíceis de obter – e talvez elas devam – mas vocês sabem o que? Isso também significa que para países como a Rússia e a China evidências digitais se tornam mais difíceis de obter – e provavelmente elas devem. Porque da maneira na qual o sistema estadunidense está funcionando, ele está recusando pedidos que podem ser usados para perseguir pessoas, perseguir dissidentes, esses pedidos simplesmente não são atendidos nesse sistema. Ele cumpre uma função protetiva valiosa para os direitos humanos. E quando eu penso em soluções que resolvem problemas e deixam as coisas mais fáceis para o procura-

dor do Brasil conseguir dados, eu também estou pensando na pessoa na China e na pessoa na Rússia que podem precisar de alguma proteção de um sistema de MLAT que funcione.

Então antes que nós cheguemos às soluções, eu gostaria de mencionar mais uma coisa: eu falei até agora sobre a entrega de conteúdo. As regras para dados que não são conteúdo nos EUA são bem diferentes. E como eu disse, você não precisa atender à causa provável, mas vocês sabem o que mais? As regras para os não-conteúdos não se aplicam para pedidos governamentais, quando o governo é um governo estrangeiro. Escutem isso: sob a lei estadunidense, se há uma demanda para dados de tráfego – quem enviou um email para quem – se essa demanda vem do Brasil ou de qualquer outro país, um provedor estadunidense pode revelar essa informação voluntariamente. Se esse pedido vem do governo estadunidense, ele não pode. Ele não pode. Ele tem que dizer ao governo estadunidense "vá conseguir uma ordem judicial" mesmo quando nós podemos revelar esses dados para qualquer outro governo no mundo, o governo estadunidense precisa de uma ordem judicial. Para mim, isso é sacana. Isso precisa ser mudado, isso não deveria ser o caso – e os dados que podem ser revelados não são apenas dados de não-estadunidenses. Se o governo do Brasil vai ao Google para conseguir o meu Gmail, o Google pode revelar essa informação para o governo do Brasil, eles não poderiam fazer isso para o governo estadunidense. Eles poderiam fazer isso para qualquer outro governo e isso parece algo que também precisa ser encarado.

PROPOSTAS DE SOLUÇÃO

Bem, eu descrevi um problema. É um dos grandes. Mas isso não vai durar porque eu acho que todos os atores no sistema acreditam que isso precisa ser resolvido. Investigações criminais que são muito importantes para a segurança pública es-

/ PARECE QUE O QUE OS ESTADOS UNIDOS ESTÃO FAZENDO É EXPORTAR A SUA PRÓPRIA LEI, CERTO? /

/ O SISTEMA DOS EUA CUMPRE FUNÇÃO VALIOSA PARA DIREITOS HUMANOS: RECUSA PEDIDOS QUE PODEM SER USADOS PARA PERSEGUIR PESSOAS. /

tão sendo obstruídas. É injusto para os provedores que estão presos no meio de regimes legais contraditórios. Eu quero dizer, as pessoas gostam de como "é difícil ter muita simpatia por uma empresa bilionária", mas elas são realmente feitas de pessoas reais, elas têm empregados, eles têm famílias e quando eles são colocados na cadeia por não cumprir um pedido é um grande problema e eu acho que nós também temos que considerar isso. Também é injusto para nós consumidores porque nós não sabemos quais leis se aplicam aos nossos dados.

Eu vou falar sobre soluções que eu acho que estão avançando mais do que as outras. Elas meio que caem em duas categorias: uma é o que eu chamo de "soluções de força bruta" e a outra são as soluções de "colaboração legal".

As soluções de força bruta – vocês sabem, alguns juízes brasileiros estão se engajando em algumas dessas – incluem prender executivos de provedores que não cumprem demandas mesmo que exista um regime legal concorrente. Elas são soluções como encerrar serviços como o WhatsApp. Forçar a localização de dados é outra solução de força bruta, [mas] que o Marco Civil rejeitou em grande parte. Hackeamento do governo, sobre o qual a Riana falou um pouco,[7] que é o governo hackeando serviços porque eles não conseguem os dados por outros meios legais, então eles usam os seus próprios meios de conseguir os dados. E a última força bruta é obrigar a implantação de backdoors na criptografia, tema sobre o qual a Riana também falou.

7. [Nota da editora] Ver texto de Riana Pfefferkorn nesse livro ou em vídeo goo.gl/XpDsDS

Todas essas soluções diminuíram de tamanho. Se você obrigar os backdoors, você deixa todo mundo menos seguro porque você faz um backdoor para os caras maus também. Se o governo está hackeando emails e enviando para você uma mensagem dizendo "clique aqui" que você acha que é de um amigo e verifica-se que é o governo tentando conseguir os seus dados insta-

lando um malware no seu dispositivo. Muito disso e as pessoas não vão mais confiar na Internet – não mais do que elas confiam agora. Obrigar a localização de dados prejudica as startups, e [o que] é ainda mais complicado, isso torna particularmente mais difícil a funcionalidade de serviços baseados em voz.

Então o que nós preferimos são soluções de maior colaboração legal. Quais são os objetivos dessas soluções? Primeiramente, proteger direitos (direitos à privacidade, direitos à liberdade de expressão) e não facilitar entregas para violadores de direitos ou em casos nos quais a própria acusação é uma violação de privacidade. Nossas soluções têm que facilitar o acesso de autoridades de investigação e isso tem que ser em escala e a escala será enorme hoje em dia e será imensa no futuro. A maior parte dos crimes, eu acho, será investigada com base em evidências digitais na medida em que nós avançamos. Será rápido, precisa ser claro e precisa ser justo no nível dos países, tem que existir uma reciprocidade. Ou seja, se um país é obrigado a viver sob regras particulares, essas regras precisam ser boas para os outros países também.

As três soluções que atingem esses critérios estão sendo discutidas agora, também se agrupam em três diferentes tipos de grupos. Existem os acordos bilaterais entre países, o que na minha visão é provavelmente a mais promissora a curto prazo. Existem as abordagens multilaterais e então temos o que eu chamo de abordagem do clube das nações. Para os bilaterais, o que acontece nos Estados Unidos à medida em que essa ideia começa a se propagar é a noção de que os EUA iriam levantar esse bloqueio na lei estadunidense que proíbe os provedores de entregarem informações para os países que as requisitam se o país requerente atinge uma série de critérios baseados em direitos humanos. Então, isso iria suplementar, mas não substituir os acordos de assistência mútua (MLAT). Isso iria funcionar da seguinte maneira: haveria uma

lei adotada nos EUA que diria "a exigência de causa provável não se aplica quando há um acordo entre os dois países"; ela permitiria o pedido [de dados]. E cada país que entra nesses acordos o faria voluntariamente, avaliando as leis do outro país e dizendo a si mesmo "nós fazemos essas leis atingirem padrões bons, fortes de direitos humanos?".

Eu devo dizer que existem certas vantagens para essa abordagem bilateral, primeiro, ela lida com o que eu chamo de o "problema da Rússia". A Rússia provavelmente tem um registro fraco de direitos humanos quando se trata de processar pessoas, mas ela também precisa resolver crimes e então você tem que ter um sistema que permita que os Russos consigam dados. Nessa ideia de um acordo bilateral, não haveria um entre os Estados Unidos e a Rússia. Os russos iriam passar pelo sistema de MLAT e seria a responsabilidade do governo estadunidense recusar o pedido que parecesse uma violação de direitos. Mas outro país, por exemplo um Brasil ou um Reino Unido, eles poderiam conseguir um acordo e fazer os pedidos diretamente para os provedores.

A maneira que eu olho para isso como um advogado de direitos humanos é que essa é uma oportunidade para aumentar padrões de pedidos de quebra de sigilo. Nós estamos olhando para coisas como incluir na lei estadunidense um requisito de devido processo legal. Teriam que haver direitos básicos de julgamento do país fazendo os pedidos, sem tortura, sem tratamento cruel e inumano, teria que haver uma forte base factual para o pedido (base factual para o crime e para acreditar que a informação sobre o crime estaria nos dados sendo procurados), autorização independente – preferencialmente por um juiz –, particularidade, que é um tipo de conceito de proporcionalidade, sem coleta em massa sob esses acordos bilaterais, notificação [ao usuário afetado] se seus dados são requisitados e entregues – isso pode acontecer depois do fato,

mas pelo menos ele seria notificado. Alguns requisitos de transparência para que as pessoas saibam com que frequência esse poder estaria sendo usado e também o processo incrível para escolha de que países teriam esses acordos bilaterais.

Os Estados Unidos, como eu acho que mencionei, já negociaram um desses acordos. Ele foi apreciado com o Reino Unido. Ele ainda não pode entrar em vigor porque a lei estadunidense que abriria o caminho para esses acordos ainda não foi introduzida ou aprovada e irá acontecer uma briga sobre quais são os padrões para esses acordos e nós iremos tentar fazer desses os padrões mais fortes que nós podemos. Até o ano passado, o Reino Unido não exigia um oficial de justiça para emitir mandados para conteúdo. Era tudo feito no nível do Secretário de Estado para Assuntos Internos, que é o equivalente do procurador chefe no país. [Mas] eles mudaram as suas leis sob a pressão de grupos de privacidade no Reino Unido e sob pressão dos Estados Unidos que queriam ter um acordo com eles, assim como eu acabei de descrever então a perspectiva de ter um desses acordos ajudou o Reino Unido a chegar à conclusão de que eles precisavam ter o envolvimento judicial nessa questão desses mandados.

Quando eu penso sobre esses acordos bilaterais, eu penso "bem, quais países vão os querer? O Brasil vai querer um" e então eu pergunto a mim mesmo e eu irei perguntar a grupos de sociedade civil no Brasil "quais são os furos na lei brasileira que precisam ser tapados, que precisam ser resolvidos nesse processo para que o Brasil possa conseguir um desses acordos?". Há um padrão bom, forte, nós sabemos qual ele é, quando as autoridades de investigação aqui querem acesso a informações em tempo real – um grampo –, mas o padrão para dados guardados talvez não é tão claro; esse é o furo. Talvez possa acontecer alguma clarificação que seria o ticket do Brasil para um desses acordos. É assim que eu estou olhando para essas coisas.

Qual é o status dessa ideia? Na semana passada houve uma audiência no Comitê Judiciário do Senado estadunidense, a ideia de acordos bilaterais foi bem recebida, o presidente do Comitê expressou um interesse em ter essa legislação até o fim do ano. Eu acho que isso é muito ambicioso. O outro corpo também teria que agir na Câmara e eu acho que nós estamos olhando para uma linha do tempo de 18 meses, ou algo assim.

Outra opção é o que eu chamo de privilégio multilateral e isso vem em maioria da Europa, isso seria um protocolo para uma convenção existente chamada Convenção de Crimes Cibernéticos de Budapeste, da qual o Brasil não faz parte, mas ele poderia ser uma parte do protocolo mesmo que não seja uma parte do próprio tratado. Esse tratado foi negociado majoritariamente entre países europeus e em sua maioria aplica-se a países europeus e estadunidenses. Ele governa com um toque sutil o acesso a dados entre fronteiras, é em sua maioria sobre processo, não sobre poder. O protocolo poderia muito bem ser sobre poder. Muitos dos defensores das liberdades civis pelo mundo criticam a Convenção de Budapeste porque ela não dá atenção suficiente aos direitos humanos, garantindo que os pedidos que ela facilita respeitem os direitos humanos. O protocolo poderia piorar o problema, mas nós não sabemos ainda quais serão os parâmetros para esse protocolo. Haverá um anúncio em algum momento no meio de junho – isso é no mês que vem – e o objetivo deles é adotar um nos próximos anos.

E finalmente, outra abordagem é o que eu chamo de abordagem do "clube das nações". Ela está sendo discutida na União Europeia em uma reunião no dia 8 de junho, quando os ministros de justiça e de assuntos internos dos estados membros irão discutir o que fazer com que ordens de produção [de dados] emitidas em um país membro da União Europeia obrigatórias em outro país, desde que o país seja avisado. Eles também estão discutindo opções não-obrigatórias e estão

olhando além das doze nações que estão na União Europeia na direção de abordagens multilaterais e bilaterais.

Então eu gostaria de deixar vocês com apenas esse pensamento. Existem opções. As opções de força bruta que estão sendo utilizadas por alguns países, a meu ver, não são muito saudáveis para a Internet e há uma perspectiva para, eu acho, outras soluções que são bilaterais, multilaterais ou clube das nações que poderiam funcionar para servir os interesses das autoridades investigação, dos defensores de direitos humanos, e dos provedores que têm que viver com essa decisão a ser feita. Muito obrigado, eu estou ansioso pelas suas questões.

PERGUNTAS/RESPOSTAS

< DENNYS ANTONIALLI > É recorrente a ideia de que há pouco interesse por parte do Departamento de Justiça dos EUA de reformar esse sistema ou de investir mais dinheiro. De fato, capacitar mais pessoas é caro e há claramente uma necessidade de priorização dos casos a serem investigados dos EUA e não casos internacionais. Na sua opinião, o que poderia gerar ou despertar algum interesse por parte do governo estadunidense em talvez investir mais nessa solução ou reestruturá-la de forma a atender as expectativas e as demandas de autoridades de outros países? É a pressão por parte de empresas estadunidenses que tem que ser feita, já que as suas subsidiárias em outros países estão passando por pressões e momentos diferentes com essas medidas drásticas? E como essas medidas drásticas repercutem no governo? Então, por exemplo, quando há o bloqueio de um aplicativo como o WhatsApp, isso repercute em algum interesse maior por parte do governo de estabelecer esses sistemas ou há algum tipo de estratégia que pode ser empreendida para que aumente o interesse nesses tipos de mecanismo nos EUA?

< GREG > Essa é uma questão muito boa. Bem, eu acho que, na verdade, o problema está menos com o Departamento de Justiça e mais com o Congresso estadunidense. É parcialmente com o Departamento de Justiça, porque eles poderiam priorizar demandas estrangeiras mais do que as demandas domésticas e isso é muito difícil para eles fazerem, por causa da pressão sob a qual eles estão. Para dar crédito a eles, o Departamento de Justiça fez duas coisas: primeiro, eles perguntaram ao congresso "ok, vamos centralizar o processamento de pedidos de MLAT vindos de governos estrangeiros. Quando o pedido de MLAT chegar ao Departamento de Justiça, nos dê a habilidade de ir a um juiz em Washington DC, ao invés de ter que ir até a Califórnia ou o estado de Washington ou Chicago, nos deixe processar em Washington DC. Nós iremos montar um grupo de procuradores muito inteligentes e eles irão ao juiz que tem muita experiência em lidar com esses pedidos de MLAT vindos de outros governos, e nós iremos fazer tudo isso em Washington". E eles conseguiram uma autoridade legal para fazer isso, mas eles não conseguiram o dinheiro que eles pediram para fazê-lo. Então o congresso disse "sim, vá em frente, ótima ideia, mas nós não vamos te dar mais dinheiro para fazer isso. Nós não vamos te dar mais pessoas e eu vou te pedir para gastar seu dinheiro em outras coisas".

Para mim esse é um problema do Congresso ao invés de um problema do Departamento de Justiça. Eles poderiam fazer coisas que eu considero como pequenas ajudas, mas eles iriam, eu acho, tornar o mundo um pouco melhor para o policial em São Paulo que cresceu aquela longa barba e está investigando esse crime: eles poderiam adotar um sistema de preenchimento eletrônico que iria estimular melhor as autoridades de investigação estrangeiras a fornecer as informações necessárias para atingir os padrões estadunidenses; eles poderiam ter um sistema de acompanhamento para que aque-

le policial que estava pensando "será que o meu pedido de MLAT será atendido?" saberia em que ponto do processo ele está; eles poderiam até dar uma estimativa de quanto tempo eles acham que irá levar para aquele MLAT ser processado; eles poderiam informar números, coisa que não fazem regularmente. (Os números que eu acabei de passar para vocês foram divulgados apenas como suporte para o pedido deles para mais dinheiro. Eu não tenho um relatório anual deles sobre o número de pedidos de MLAT que eles fazem ou o número que eles recebem. E não há uma contabilidade pública sobre o tamanho do acúmulo. Nós sabemos que o acumulado são milhares de pedidos de MLAT mas eles não divulgam isso, nós não sabemos quais são esses números). Então eu acho que existem algumas coisas que eles poderiam fazer, mas eles não vão resolver o grande problema.

< PERGUNTA > Boa noite, meu nome é Pedro, eu sou estudante de direito também, mas na PUC. Você falou muito sobre cooperação internacional, etc. Só que eu queria, por um lado dar a bola para você cortar sobre o assunto do Snowden que você queria falar e também perguntar sobre o *Patriot Act*, que permitiu, aliás permite, que o governo estadunidense faça interceptações com um processo legal diferente do que você mencionou e eu queria saber como ele funciona e como ele pode ser usado para atacar ativistas e pessoas como o Snowden?

< GREG > O *USA Patriot Act* foi decretado logo após os ataques de 11/09 e ele tem uma série de diferentes dispositivos. Muitos deles não são realmente relevantes para o que nós estamos falando hoje, alguns dos dispositivos mais desaprováveis do Patriot Act estão relacionados aos imigrantes e havia um dispositivo que permitia que o governo detivesse uma pessoa que está chegando nos EUA por sete dias sem explicação, o que não é permitido na Constituição. Em outros, ele afrouxou as regras ao redor da vigilância: ele promulgou um dos estatutos,

seção 215, que era a base legal para algumas das revelações que o Edward Snowden fez. Elas foram revelações sobre a coleta de registros telefônicos nos EUA, mas penso que o *Patriot Act* – em comparação a outro estatudo do qual já vou falar – não tem muito impacto em pessoas fora dos Estados Unidos.

Existia essa outra lei que foi decretada, o *Foreign Intelligence Surveillance Act*. A seção 702 dessa lei é a que autoriza o governo a vigiar pessoas fora dos EUA sem uma ordem judicial, sem um mandado e apenas baseado na coleta de informações relevantes para a política externa. Na verdade, essa lei expira no final desse ano, ela será reautorizada e nós vamos lutar por quais reformas a lei irá passar em conexão com esse debate da reautorização.

Um grande desenvolvimento que aconteceu semana passada foi que 30 das maiores empresas de tecnologia nos EUA apoiaram uma pauta de reforma substancial e a parte mais substancial disso é dizer que essa vigilância só pode ser conduzida por boas razões como para prevenir terrorismo, prevenir sabotagem, espionagem, ataques em forças estadunidenses e aliadas. Então isso realmente foi, eu acho, uma declaração importante de algumas dessas empresas de tecnologia. Nós, grupos das liberdades civis, vamos dizer isso o tempo inteiro, mas ter as empresas de tecnologia saindo e dizendo a mesma coisa foi muito útil e eu acho que será muito importante para esse debate.

< PERGUNTA > Boa noite, meu nome é Artur Pericles, eu sou estudante de mestrado aqui na faculdade. Minha pergunta tem a ver mais com o assunto que a gente estava discutindo. Eu queria saber o que você pensa sobre o problema da coleta de dados nas fronteiras, quando as pessoas estão chegando de avião nos EUA, da nova política a respeito disso, de exigir que as pessoas desbloqueiem os celulares para que os agentes da imigração possam examiná-los.

< GREG > Eu acho que é um desastre. Isso afeta não-cidadãos que estão visitando os EUA, isso os torna menos propensos a visitar. Existem conferências que foram movidas para fora dos EUA por causa dessas exigências. Isso também enfraquece o uso das pessoas das próprias ferramentas de comunicação que os tornaram mais produtivos e mais integrados à sociedade. Eu realmente acho que é um movimento desastroso para os EUA e eu estou realmente preocupado com outros países que irão seguir. E isso não se aplica apenas a não-cidadãos entrando, [mas também] para cidadãos quando estamos na fronteira. [Nessa situação,] nós não temos os mesmos direitos constitucionais – nós temos os mesmos direitos, mas existem mais exceções neles quando estamos entrando nos EUA. A minha organização exigiu que todos os viajantes internacionais deletem suas contas de email antes de retornar aos EUA; nós os reinstalamos uma vez que entramos de volta, mas nós temos que deletá-los quando nós retornamos e a ideia é que nós não queremos que o governo tenha acesso às nossas comunicações mesmo que nós não estejamos fazendo nada de errado, e eu devo dizer que como um estadunidense isso realmente me machuca especialmente porque é o meu governo fazendo isso comigo e não há muito o que se pode fazer sobre isso.

Existem desafios pendentes nisso, e eu sei que a Electronic Frontier Foundation (EFF) está ativamente procurando por mais casos. Eu não sei exatamente onde eles vão parar, mas eu antecipo que esse problema irá piorar porque nós temos o Sr. Trump falando sobre extrema segurança [*extreme vetting*]. A sua primeira ordem de extrema segurança foi segurada pelos tribunais, a segunda também, mas eles estão procurando mais e mais maneiras de fazê-lo e eles estão olhando para as senhas de mídias sociais, essa é uma coisa que eles podem pedir.

ESTE LIVRO FOI COMPOSTO COM AS FAMÍLIAS TIPOGRÁFICAS *DÉCIMA MONO* E *META*. O PROJETO GRÁFICO É DE AUTORIA DO *ESTÚDIO CLARABOIA* E AS ILUSTRAÇÕES SÃO DA *PINGADO SOCIEDADE ILUSTRATIVA*. FORAM IMPRESSAS XXX COPIAS PELA GRÁFICA XXX EM MAIO DE 2018

Agência Brasileira do ISBN
ISBN 978-85-92871-01-7

INTERNETLAB
pesquisa em direito e tecnologia